NETCOMM GATEWAY™ SERIES

ADSL2+ Wireless N300 Modem Router with VoIP

USER GUIDE

Preface

This manual provides information related to the installation, operation, and application of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be broken or malfunctioning, please contact technical support for immediate service by email at technicalsupport@netcomm.com.au

For product update, new product release, manual revision, or software upgrades, please visit our website at http://www.netcomm.com.au

Important Safety Instructions

With reference to unpacking, installation, use and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.

CAUTION:

- To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.

WARNING

- Disconnect the power line from the device before servicing.

Copyright

Copyright©2008 NetComm Limited. All rights reserved. The information contained herein is proprietary to NetComm Limited. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of NetComm Limited.

NOTE:This document is subject to change without notice.

Save Our Environment

When the equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste. You may be subject to penalties or sanctions under the law. Instead, ask for disposal instructions from your municipal government.

Please be responsible and protect our environment.

Table of Contents

1 INTRODUCTION 5
1.1 Features 6
1.2 Application 7
1.3 Front Panel Led Indicators 7
2 INSTALLATION 8
2.1 Hardware Installation 9
2.2 Configuring Your Computer 9
3 WEB USER INTERFACE 10
3.1 Login Procedure 11
3.2 Default Settings 11
4 QUICK SETUP 12
4.1 Auto Quick Setup 13
4.2 Manual Quick Setup 14
4.2.1PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE) 15
4.2.2MAC Encapsulation Routing (MER) 18
4.2.3IP Over ATM 20
4.2.4Bridging 22
5. VOICE 25
5.1 SIP 26
5.1.1 SIP Basic 26
5.1.2 SIP Advanced 27
5.1.3 SIP Debug 28
5.2 Telephone Calls 28
6. WIRELESS 30
6.1 Setup 31
6.2 Wireless Security Quick Setup 32
6.3 Wireless Security in Detail 33
6.4 Configuration 36
6.5 Mac Filter 37
6.6 Wireless Bridge 38
6.7 Station Info 38
7. MANAGEMENT 39
7.1 Device Settings 40
7.1.1 Backup 40
7.1.2 Update 40
7.1.3 Restore Default 40
7.1.4 Update Firmware 40
7.2 SNMP 41
7.3 TR-069 42
7.4 SNTP 42
7.5 Access Control 43
7.5.1 Services 43
7.5.2 Access IP Adresses 43
7.5.3 Passwords 43
7.6 Save and Reboot 44
8. ADVANCED 45
8.1 WAN 46
8.1.1 VLAN MUX 46
8.1.2 MSP 47
8.2 LAN 49
8.3 QoS Classification 50
8.3.1 Queue Management Configuration 50
8.3.2 QoS Queue Configuration 50
8.3.3 QoS Classification 51
8.4 Routing 52
8.4.1 Default Gateway 52
8.4.2 Static Route 52
8.5 DSL 53
8.6 Port Mapping 54
9. STATUS 55
9.1 Diagnostics 56
9.2 System Log 56
9.3 WAN 58

9.4 Statistics 58
9.4.1 LAN Statistics 58
9.4.2 WAN Statistics 59
9.4.3 ATM Statistics 59
9.4.4 ADSL Statistics 60
APPENICIES 62
APPENDIX A: LEGAL AND REGULATORY INFORMATION 63

Introduction

Get To Know Your Product

Introduction

The NetComm **NB9WMAXXn ADSL2+ Wireless N Modem Router with VoIP** is a true all-in-one device that combines a number of technologies, eliminating the need to clutter your desk with many separate devices.

Connect to the Internet with ADSL2+, share the connection with built-in Wireless N or 4 LAN Ethernet ports and utilise the VoIP ports to make phone calls over the Internet, drastically reducing your phone bills.

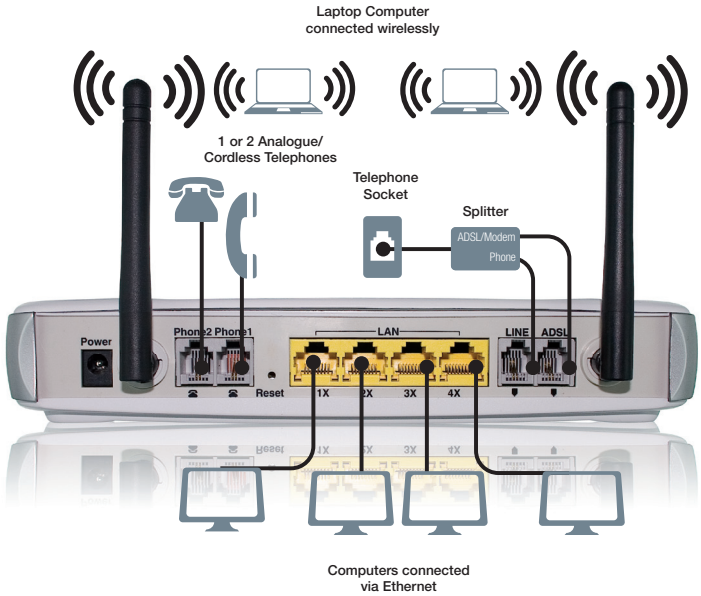
Ideal for home and SOHO environments that require an Internet signal to be networked among multiple users and who would benefit from the cost saving opportunity that VoIP can provide. The NB9WMAXXn is the perfect backbone for home and office Internet connectivity.

1.1 Features

- Fully featured ADSL2+ modem router
- Annex M supported
- Wireless N for speeds of up to 300Mbps
- Integrated VoIP ATA with two phone ports
- 4 x 10/100 LAN ports for wired connections
- FXO “Lifeline” port for regular PSTN calls
- Layer 3 QoS to ensure VoIP call quality
- Supports advanced call services – caller ID, call on-hold, call forwarding, call waiting and transfer
- VPN pass-through
- Advanced security features

1.2 Application

The diagram below depicts a typical application of the **NB9WMAXXn** series.



1.3 Front Panel LED Indicators

The front panel LED indicators are shown and explained below.

LED	Colour	Mode	Function
POWER	Green	On	The router is powered up
		Off	The router is powered down
ADSL	Green	On	The ADSL Link is established
		Off	The ADSL Link is not established
	Green	Blink	The ADSL line is training or traffic is passing through
LINE	Green	On	FXO (Pass through) Line is off hook
		Off	FXO Line is on hook
PHONE1	Green	On	FXS (VoIP) Phone 1 is off hook
		Off	FXS Phone 1 is on hook
PHONE2	Green	On	FXS Phone 2 is off hook
		Off	FXS Phone 2 is on hook
LAN 1x ~4x	Green	On	Ethernet link is established
		Off	Ethernet link is not established
	Green	Blink	Data transmitting/receiving over Ethernet
WLAN	Green	On	Wireless is ready
		Off	Wireless is disabled
	Green	Blink	Data transmitting/receiving over Wireless
Internet	Red	On	Device attempted to obtain an IP address and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.) For bridged mode, this LED remains off. If the IP or PPPoE session is dropped due to an idle timeout, the LED will remain green if an ADSL connection is still present. If the session is dropped for any other reason, the LED is turned off. The LED will turn red when it attempts to reconnect and DHCP or PPPoE fails.
		Off	Modem is in bridged mode or ADSL connection not present.
	Green	Blinking	IP connected and data is passing through the device (either direction)

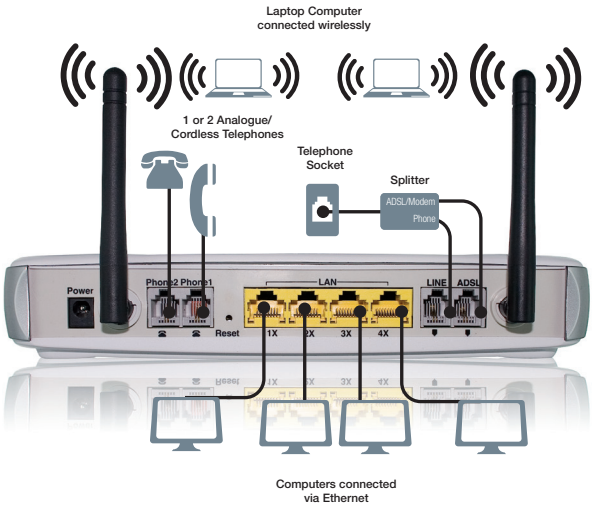
Installation

Connecting Your Device

Installation

2.1 Hardware Installation

Follow the instructions below to complete the hardware installation.



Connection to ADSL port

Connect to an ADSL2/2+ service with this RJ11 Port. This device contains a micro filter which removes the analog phone signal. If you wish, you can connect a regular telephone to the same line by using a POTS splitter.

Connection to LAN ports

To connect to a hub or PC, use RJ45 Ethernet cable. You can connect the router to four LAN devices. The ports are auto-sensing MDI/X and either straight-through cable or crossover cable can be used.

Connection to Phone ports

Connect up tp two standard analogue phones with an RJ11 cable to utilise a VoIP service

Connection to Power

Connect the power jack to the shipped power cord. Attach the power adapter to the wall outlet or other AC source. After powering on, the router will perform a self-test. Wait a few moments and the router will be ready to operate.

Caution 1: If the router fails to power up, or if it malfunctions, first verify that the power supply is connected correctly. Then power it on again. If the problem persists, contact our technical support engineers.

Caution 2: Before servicing or disassembling this equipment always disconnect all power cords and telephone lines from the wall outlet.

Reset Button

In the back panel, there is a reset button. Restore the default parameters of the device by holding down this button until the front panel LED indicators start blinking simultaneously (about 10 seconds). If held down longer, the device may go into a firmware update state (CFE boot mode). The user can then update the device from any web browser using the default IP address (http://192.168.1.1) without login.

2.2 Configuring your Computer

PC Network Adapter setup (Windows XP)

Set your network adapter to obtain an IP Address automaticly (See section on PC Network Adapter setup in this manual for details)

- Click on [Start Menu] > select [Control panel] > select [Network Connections]
- Select [Local Area Connection]) icon > select [properties]
- Select [Internet Protocol (TCP/IP)] > Click [Properties]
- Select the [General] tab
- Please select both
  - Obtain an IP address automatically
  - Obtain DNS server address automatically

Web User Interface

Where You Go To Set Up Your Device

Web User Interface

This section describes the setup procedure to access the web user interface.

3.1 Login Procedure

Follow these steps to login to the web user interface.

1: Open an Internet browser (e.g. Microsoft Internet Explorer) and enter the default IP address for the router in the URL address field at top. For example, if the IP address is 192.168.1.1, enter "http://192.168.1.1".

2: Next, you will be prompted to enter your user name and password. Enter **admin** as the user name and **admin** as the password, and then click **OK**. These values can be changed later (see section 8.5.3).

Connect to 192.168.1.1
The server 192.168.1.1 at NB9WMAXXn requires a username and password.
Warning: This server is requesting that your username and

3: After successfully logging in, you will reach the Quick Setup menu.

3.2 Default Settings

The following list shows the factory default settings for this router.

- LAN port IP address: 192.168.1.1
- Local administrator account name: admin
- Local administrator account password: admin
- Local non-administrator account name: user
- Local non-administrator account password: user
- Remote WAN access: disabled (except for ICMP)
- Remote WAN access account name: support
- Remote WAN access account password: support
- NAT and firewall:Disabled for MER, IPoA and Bridge modes Enabled for PPPoE and PPPoA modes
- DHCP server on LAN interface: enabled
- WAN IP address: none
- Wireless access: enabled
- SSID: Netcomm Wireless
- Wireless authentication: enabled Password a1b2c3d4e5
- Annex A enabled / Annex M disabled

This router supports the following connection types.

- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoA)
- MAC Encapsulated Routing (MER)
- IP over ATM (IPoA)
- Bridging

Technical Note:

During power on, the device initializes all settings to default values. It will then read the configuration profile from the permanent storage section of flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile in permanent storage can be created via the web user interface or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than five seconds until the power indicates LED blinking or by clicking the Restore Default Configuration option in the Restore Default screen, section 8.1.3.

Quick Setup

Follow a few short steps to begin

Quick Setup

The Quick Setup screen allows the user to configure the router for DSL connectivity and Internet access. It also guides the user though the WAN network setup first and then the LAN interface setup. You can either manually customize the router or follow the online instruction to set up the router.

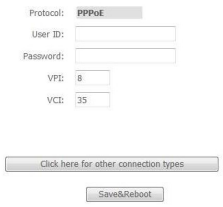
The following configuration considerations apply:

- The WAN network operating mode operation depends on the service provider's configuration in the Central Office and Broadband Access Server for the PVC
- If the service provider provides PPPoE service, then the connection selection depends on whether the LAN-side device (typically a PC) is running a PPPoE client or whether the router is to run the PPPoE client. The router can support both cases simultaneously.
- If some or none of the LAN-side devices do not run PPPoE client, then select PPPoE. If every LAN-side device is running a PPPoE client, then select Bridge In PPPoE mode, the router also supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices. In most cases, NAT and firewall should always be enabled when PPPoE or PPPoA mode are selected, but they can be enabled or disabled by the user when MER or IPoA is selected, NAT and firewall are always disabled when Bridge mode is selected.
- Depending on the network operating mode, and whether NAPT and firewall are enabled or disabled, the main panel will display or hide the NAPT/Firewall menu. For instance, at initial setup, the default network operating mode is Bridge. The main panel will not show the NAPT and Firewall menu.

NOTE: Up to sixteen PVC profiles can be configured and saved on the flash memory. To activate a particular PVC profile, you must navigate through all the Quick Setup screens until the last summary screen, and then click on the Save/Reboot button.

4.1 Auto Quick Setup

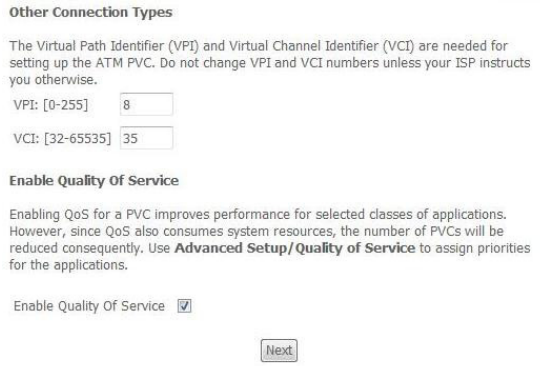
The auto quick setup requires the DSL link to be up. The router will automatically detect the best connection type. You need only to follow the online prompts.



1. For PPPoE connections, simply enter your User ID and Password as provided by your ISP, then click Save & Reboot. For other connection types, click on **Click Here for Other Connection Types** and follow the instructions to complete the setup.
2. After the process is complete, you can use the DSL service.

4.2 Manual Quick Setup

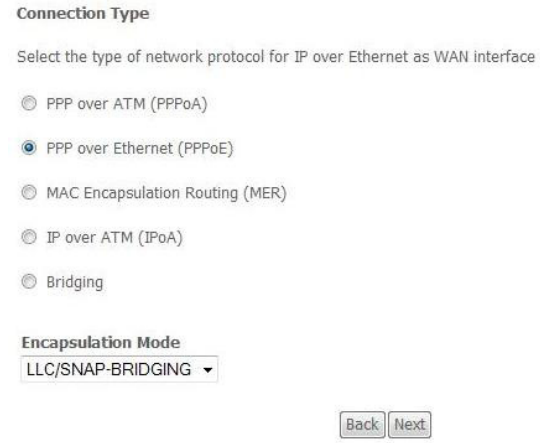
Click on **Click here for other Connection Types** to display the folowing screen.


Other Connection Types
The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not change VPI and VCI numbers unless your ISP instructs you otherwise.
VPI: [0-255] 8
VCI: [32-65535] 35
Enable Quality Of Service
Enabling QoS for a PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service
Next

1. Enter the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) values. Select Enable Quality of Service if required and click Next.
2: Choose a Connection Type and Encapsulation Mode.

Choosing different connection types provides different encapsulation modes.

- PPPoA- VC/MUX, LLC/ENCAPSULATION
- PPPoE- LLC/SNAP BRIDGING, VC/MUX
- MER- LLC/SNAP-BRIDGING, VC/MUX
- IPoA- LLC/SNAP-ROUTING, VC MUX
- Bridging- LLC/SNAP-BRIDGING, VC/MUX

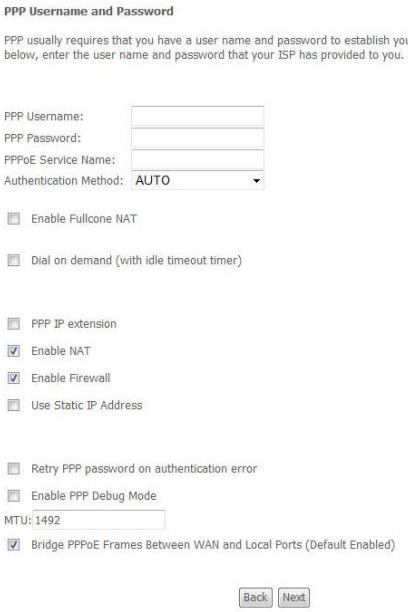


NOTE: The sections that follow describe the PVC setup procedure further. Choosing different connection types pops up different settings requests. Enter appropriate settings that are required by your service provider.

4.2.1 PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE)

Follow Steps 1 through to 3 of Manual Quick Setup

4: Select the PPP over ATM (PPPoA) or PPP over Ethernet (PPPoE) radio button and click Next. The following screen appears.


PPP Username and Password
PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.
PPP Username:
PPP Password:
PPPoE Service Name:
Authentication Method: AUTO
Enable Fullcone NAT
Dial on demand (with idle timeout timer)
PPP IP extension
Enable NAT
Enable Firewall
Use Static IP Address
Retry PPP password on authentication error
Enable PPP Debug Mode
MTU: 1492
Bridge PPPoE Frames Between WAN and Local Ports (Default Enabled)
Back
Next

PPP Username/PPP Password

The PPP Username and the PPP password requirements are dependent on the particular requirements of the ISP or the DSL service provider. The web user interface allows a maximum of 256 characters for the PPP username and a maximum of 32 characters for PPP password.

Enable Fullcone NAT

Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

Dial on Demand

The router can be configured to disconnect if there is no activity for a period of time by selecting the Dial on demand check box. When the checkbox is ticked, you need to enter the inactivity timeout period. The timeout period ranges from 1 minute to 4320 minutes.

PPP IP Extension

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specially requires this setup, do not select it.

The PPP IP Extension supports the following conditions:

- Allows only one PC on the LAN
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the router has a single IP address to assign to a LAN device.
- NAT and firewall are disabled when this option is selected.
- The router becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The router extends the IP subnet at the remote service provider to the LAN PC. That is, the PC becomes a host belonging to the same IP subnet.
- The router bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the router's LAN IP address.

Enable NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side, this checkbox should be de-selected to free up system resources for better performance. When the system comes back after reboot, the NAT submenu will be gone.

Enable Firewall

If the firewall checkbox is selected, the Security submenu will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will be gone.

Use Static IP Address

Unless your service provider specially requires this setup, do not select it.

If selected, enter your static IP address.

Retry PPP password on authentication error

Tick the box to select.

Enable PPP Debug Mode

Enable the PPPoE debug mode. The system will put more PPP connection information in System Log. But this is for debug, please don't enable in normal usage.

Bridge PPPoE Frames Between WAN and Local Ports (Default Enabled)

If Enabled, the function can create a local PPPoE connection to the WAN side."

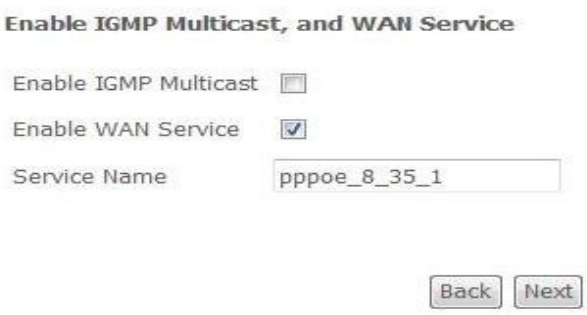
(PPPoE only) Bridge PPPoE Frames Between WAN and Local Ports (Default Enabled)

If Enabled, the function can create a local PPPoE connection to the WAN side.

Bridge PPPoE Frames Between WAN and Local Ports (Default Enabled)

If Enabled, the function can create a local PPPoE connection to the WAN side.

5: Click **Next** to display the following screen.



Enable IGMP Multicast checkbox:

Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

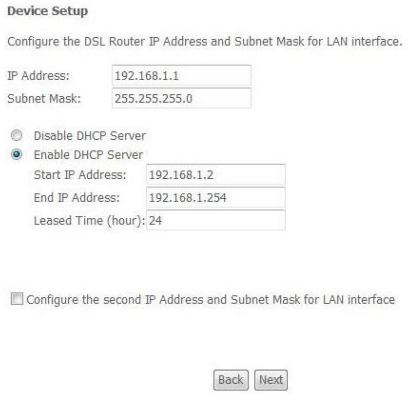
Enable WAN Service checkbox:

Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name:

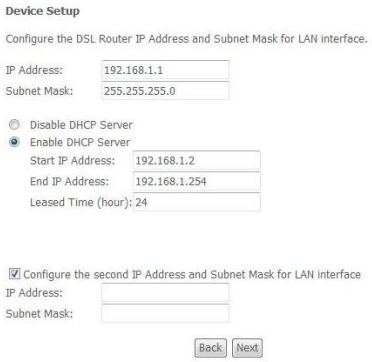
This is user-defined.

6: After entering your settings, select Next. The following screen appears.


Device Setup
Configure the DSL Router IP Address and Subnet Mask for LAN interface.
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Disable DHCP Server
Enable DHCP Server
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Leased Time (hour): 24
Configure the second IP Address and Subnet Mask for LAN interface
Back
Next

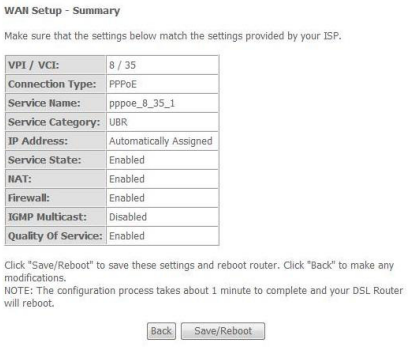
This screen allows the user to configure the LAN interface IP address, subnet mask and DHCP server. If the user would like this router to assign dynamic IP address, DNS server and default gateways to other LAN devices, select the button Enable DHCP server and enter the Start and End IP addresses and DHCP leased time.

To configure a secondary IP address for the LAN port, tick the checkbox shown.



7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown), input a new SSID (if desired) and click Next.

8: Click Next to display the WAN Setup-Summary screen that presents the entire configuration summary. Click Save/Reboot if the settings are correct. Click Back if you wish to modify the settings.

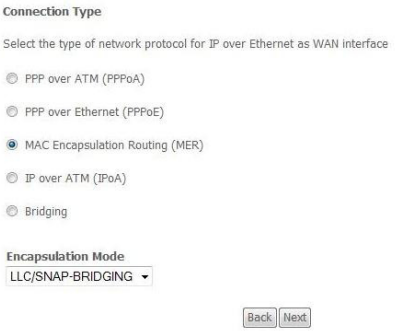

WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
VPI / VCI: 8 / 35
Connection Type: PPPoE
Service Name: pppoe_8_35_1
Service Category: UBR
IP Address: Automatically Assigned
Service State: Enabled
NAT: Enabled
Firewall: Enabled
IGMP Multicast: Disabled
Quality Of Service: Enabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back
Save/Reboot

9: After clicking Save/Reboot, the router will save the configuration to flash memory and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Home screen automatically. The router is ready for operation when the LED indicators display as described in Section 1.3

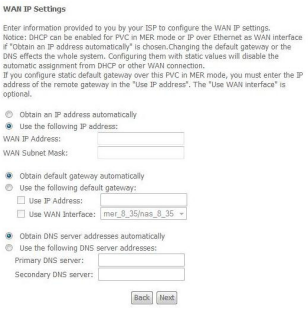
4.2.2 MAC Encapsulation Routing (MER)

Follow Steps 1 through to 3 of Manual Quick Setup

4: Select the MAC Encapsulation Routing (MER) radio button and click Next.



The following screen appears.


WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen.Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.
If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.
Obtain an IP address automatically
Use the following IP address:
WAN IP Address:
WAN Subnet Mask:
Obtain default gateway automatically
Use the following default gateway:
Use IP Address:
Use WAN Interface:
mer_8_35/nas_8_35
Obtain DNS server addresses automatically
Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:
Back
Next

Enter information provided to you by your ISP to configure the WAN IP settings.

NOTE: DHCP can be enabled for PVC in MER mode if Obtain an IP address automatically is chosen. Changing the default gateway or the DNS affects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.

If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address" field. The ISP will provide the values to enter in these fields.

5: Click **Next** to display the following screen.

Network Address Translation Settings
Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).
Enable NAT
Enable Fullcone NAT
Enable Firewall
Enable IGMP Multicast, and WAN Service
Enable IGMP Multicast
Enable WAN Service
Service Name:
mer_0_8_35
Back
Next

Enable NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side, this checkbox should be de-selected to free up system resources for better performance. When the system comes back after reboot, the NAT submenu will be gone.

Enable Firewall

If the firewall checkbox is selected, the Security submenu will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will be gone.

Enable IGMP Multicast

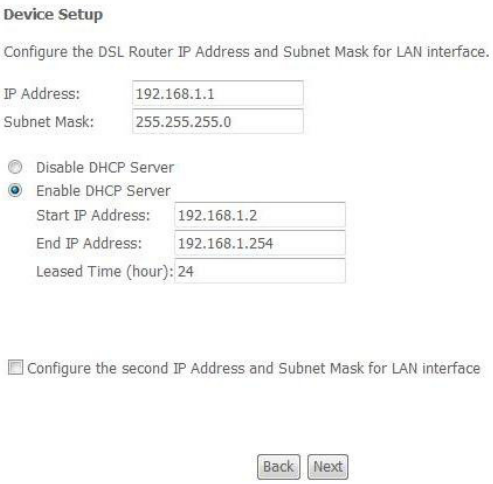
Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service

Tick the checkbox to enable the WAN service. If this item is not selected, you will not be able to use the WAN service.

Service Name: This is User-defined.

6: Upon completion click **Next**. The following screen appears.


Device Setup
Configure the DSL Router IP Address and Subnet Mask for LAN interface.
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Disable DHCP Server
Enable DHCP Server
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Leased Time (hour): 24
Configure the second IP Address and Subnet Mask for LAN interface
Back
Next

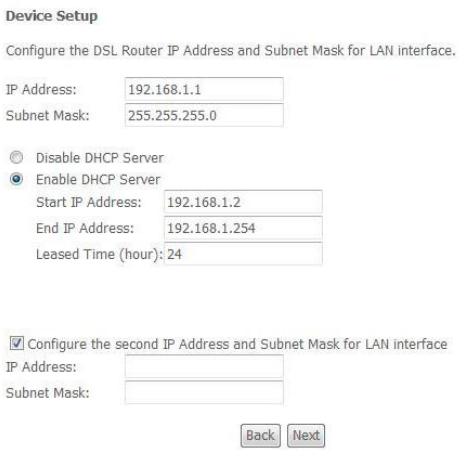
Consult the following paragraphs for more details about these settings.

The Device Setup screen allows the user to configure the LAN interface IP address and DHCP server. If the user would like this router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices, select the radio box **Enable DHCP** server to enter the starting IP address and end IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from the remote DHCP server. The remote DHCP server will provide the IP address.

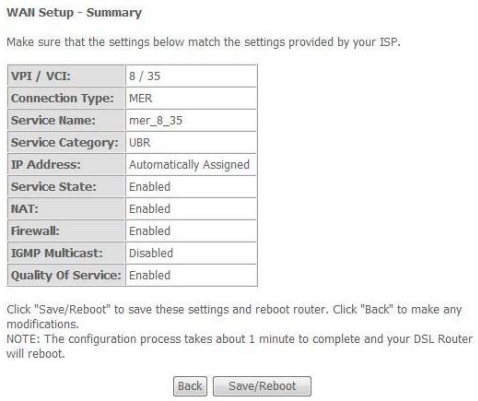
NOTE: If NAT is enabled, Enable DHCP Server Relay won't display.

To configure a secondary IP address for the LAN port, tick the checkbox shown.



7: Click Next to continue. To enable the wireless function, tick the checkbox (as shown), input a new SSID (if desired) and click Next**.**

The following screen will display.


WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
VPI / VCI: 8 / 35
Connection Type: MER
Service Name: mer_8_35
Service Category: UBR
IP Address: Automatically Assigned
Service State: Enabled
NAT: Enabled
Firewall: Enabled
IGMP Multicast: Disabled
Quality Of Service: Enabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back
Save/Reboot

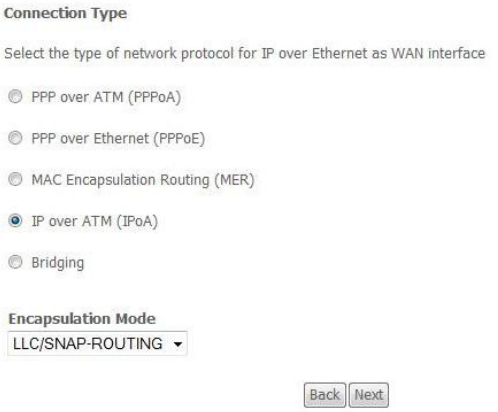
8: The WAN Setup-Summary screen presents the entire configuration summary. After clicking Save/Reboot, the router will save the configuration to flash memory and reboot. Click Back if you wish to modify the settings. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Home screen automatically. The router is ready for operation when the LED indicators display as described in Section 1.3

4.2.3 IP Over ATM

Follow Steps 1 through to 3 of Manual Quick Setup

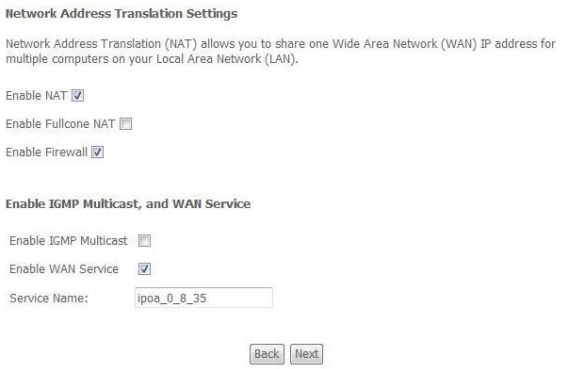
4: Select the IP over ATM (IPoA) radio button and click **Next**.

The following screen appears.



NOTE: DHCP is not supported over IPoA. The user must enter the IP address or WAN interface for the default gateway setup and the DNS server addresses provided by the ISP.

5: Click **Next**. The following screen appears.


Network Address Translation Settings
Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).
Enable NAT
Enable Fullcone NAT
Enable Firewall
Enable IGMP Multicast, and WAN Service
Enable IGMP Multicast
Enable WAN Service
Service Name:
ipoa_0_8_35
Back
Next

Enable NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox should be de-selected. When the system comes back after reboot, the NAT submenu will be no longer available.

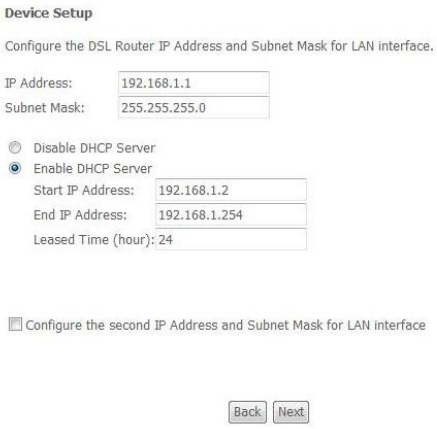
Enable Fullcone NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

Enable Firewall

If the firewall checkbox is selected, the Security submenu will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will be gone.

6: Click **Next** to display the following screen.


Device Setup
Configure the DSL Router IP Address and Subnet Mask for LAN interface.
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Disable DHCP Server
Enable DHCP Server
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Leased Time (hour): 24
Configure the second IP Address and Subnet Mask for LAN interface
Back
Next

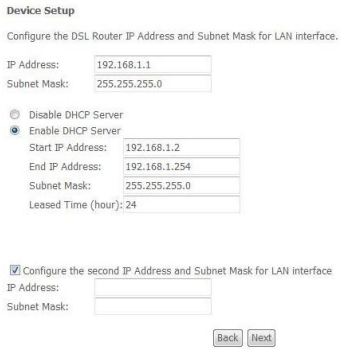
The Device Setup screen allows the user to configure the LAN interface IP address and DHCP server. If the user would like this router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices. Select the button Enable DHCP server on the LAN to enter the starting IP address and end IP address and DHCP lease time.

The Device Setup screen allows the user to configure the LAN interface IP address and DHCP server. If the user would like this router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices. Select the radio box **Enable DHCP server on the LAN** to enter the starting IP address and end IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from the remote DHCP server. The remote DHCP server will provide the IP address.

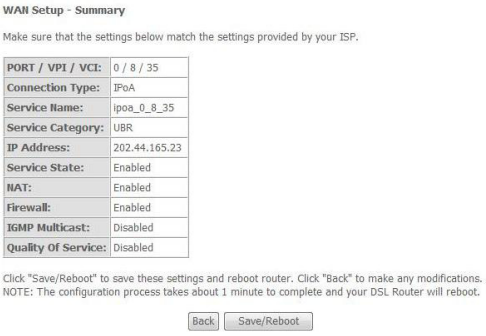
NOTE: If NAT is enabled, Enable DHCP Server Relay won't display.

To configure a secondary IP address for the LAN port, click the box as shown below.


Device Setup
Configure the DSL Router IP Address and Subnet Mask for LAN interface.
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Disable DHCP Server
Enable DHCP Server
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0
Leased Time (hour): 24
Configure the second IP Address and Subnet Mask for LAN interface
IP Address:
Subnet Mask:
Back Next

7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown), input a new SSID (if desired) and click **Next**.

The following screen will be displayed.

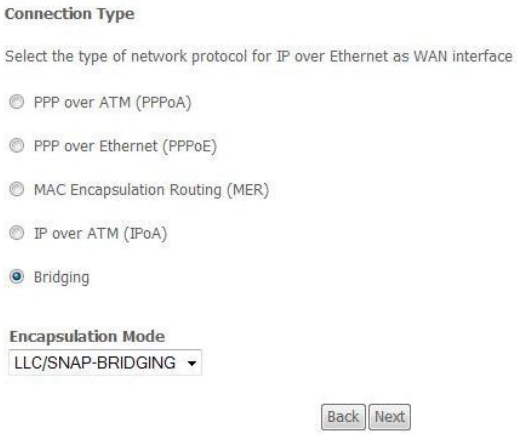

WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
PORT / VPI / VCI: 0 / 8 / 35
Connection Type: IPoA
Service Name: ipoa_0_8_35
Service Category: UBR
IP Address: 202.44.165.23
Service State: Enabled
NAT: Enabled
Firewall: Enabled
IGMP Multicast: Disabled
Quality Of Service: Disabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back Save/Reboot

8: The WAN Setup-Summary screen presents the entire configuration summary. After clicking Save/Reboot, the router will save the configuration to flash memory and reboot. Click Back if you wish to modify the settings. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Home screen automatically. The router is ready for operation when the LED indicators display as described in Section 1.3

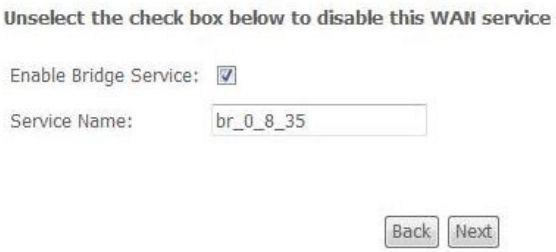
4.2.4 Bridging

Follow Steps 1 through to 3 of Manual Quick Setup

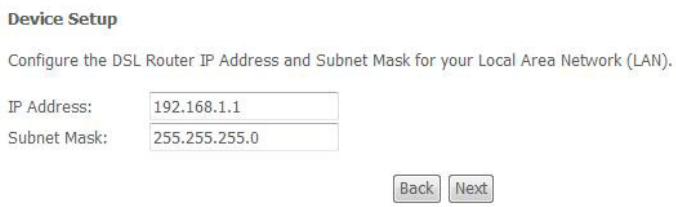
4: Select the Bridging radio button and click **Next**.



The following screen appears. To use the bridge service, tick the **Enable Bridge Service** checkbox and enter a service name (user defined).

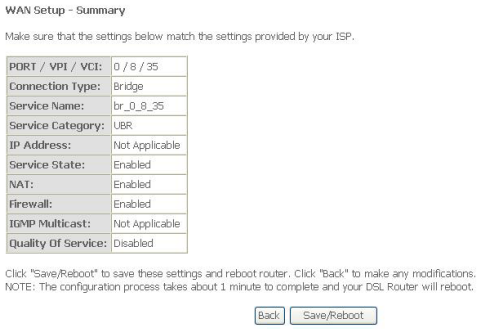


5: Click the **Next** button to continue. Enter the IP address for the LAN interface. The default IP address is 192.168.1.1. The LAN IP interface in bridge operating mode is needed for local users to manage the router. Notice that there is no IP address for the WAN interface in bridge mode, and technical support cannot access the router remotely.



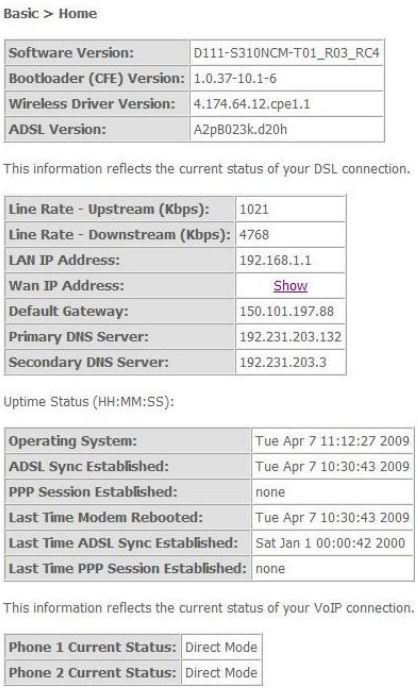
6: Click **Next** to continue. To enable the wireless function, select the radio button (as shown), input a new SSID (if desired) and click **Next**.

The following screen will be displayed.


WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
PORT / VPI / VCI: 0 / 8 / 35
Connection Type: Bridge
Service Name: br_0_8_35
Service Category: UBR
IP Address: Not Applicable
Service State: Enabled
NAT: Enabled
Firewall: Enabled
IGMP Multicast: Not Applicable
Quality Of Service: Disabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back
Save/Reboot

7: The WAN Setup-Summary screen presents the entire configuration summary. After clicking **Save/Reboot**, the router will save the configuration to the flash memory, and reboot. Click **Back** if you wish to modify the settings. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the **Device Info** screen automatically.

Select **Basic Info** from the main menu to display Summary information as below.



Basic > Home

Software Version:	D111-S310NCM-T01_R03_RC4
Bootloader (CFE) Version:	1.0.37-10.1-6
Wireless Driver Version:	4.174.64.12.cpe1.1
ADSL Version:	A2pB023k.d20h

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	1021
Line Rate - Downstream (Kbps):	4768
LAN IP Address:	192.168.1.1
Wan IP Address:	Show
Default Gateway:	150.101.197.88
Primary DNS Server:	192.231.203.132
Secondary DNS Server:	192.231.203.3

Uptime Status (HH:MM:SS):

Operating System:	Tue Apr 7 11:12:27 2009
ADSL Sync Established:	Tue Apr 7 10:30:43 2009
PPP Session Established:	none
Last Time Modem Rebooted:	Tue Apr 7 10:30:43 2009
Last Time ADSL Sync Established:	Sat Jan 1 00:00:42 2000
Last Time PPP Session Established:	none

This information reflects the current status of your VoIP connection.

Phone 1 Current Status:	Direct Mode
Phone 2 Current Status:	Direct Mode

NOTE: The figure above shows the summary screen with an ADSL signal.

For more information on ADSL Quick Setup, please refer to Chapter 4- Quick Setup

Voice

Set Up Your VoIP Connection

Voice

This chapter first describes the various options for configuration of the SIP voice service. It then provides detailed instructions for making telephone calls using VoIP (Voice over IP) or PSTN (Public Switched Telephone Network) services

5.1 SIP

Session Initiation Protocol (SIP) is a peer-to-peer protocol used for Internet conferencing, telephony, events notification, presence and instant messaging.

SIP is designed to address the functions of signalling and session management within a packet telephony network. Signalling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

The SIP standard defines the following agents/servers:

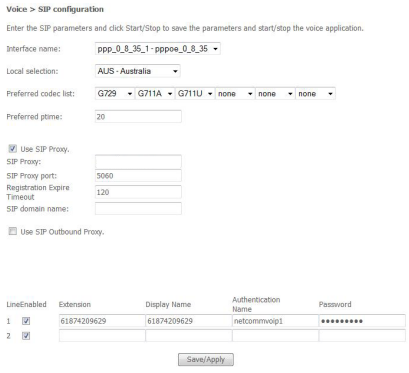
1. User Agents (UA) - SIP phone clients (hardware or software)
2. Proxy Server – relays data between UA and external servers
3. Registrar Server - a server that accepts register requests from UA
4. Redirect Server – provides an address lookup service to UA

NOTE: The SIP standard is set by the Internet Engineering Task Force (IETF).

The following subsections present Basic, Advanced and Debug SIP screens. Each screen provides various options for customizing the SIP configuration.

5.1.1 SIP BASIC

This screen contains basic SIP configuration settings.



Once settings are configured click **Save/Apply** to begin using the service.

NOTE: Consult the tables that follow for detailed field descriptions

Interface name	Choose the WAN interface
Locale Selection	Sets tone, ring type and physical characteristics for specific countries
Preferred codecs	Choose G.711U, G.711A, G.726 or G.729
Preferred ptime	The time period used to digitally sample the analog voice signal. The default is 20 ms.

Use SIP proxy	Enable the SIP proxy by selecting the checkbox and setting proxy parameters.
SIP Proxy	Input IP address or domain name of the SIP proxy server, used for VOIP service.
SIP Proxy port	This value is set by your VoIP provider and is normally port 5060.
Registration Expire Timeout	The time period the user would like the registration to be valid for the Registrar/ Proxy Server. The default is 300 seconds.
SIP domain name	Provided by your VoIP provider.

- A proxy is an intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or transferred to other servers. A proxy interprets and, if necessary, rewrites a request message before forwarding it

Use SIP outbound proxy	Select if required by your VoIP provider. Enter SIP Outbound proxy IP and port.

Line 1 & 2	Ports FXS1 & FXS2
Disabled	Ticking the checkbox disables the line
Extension	The line extension number
Display Name	The caller ID display name
Authentication Name	The authentication username for the Registrar/Proxy, given by VOIP provider.
Authentication Password	The authentication password for the Registrar/proxy, given by VOIP provider.

5.1.2 SIP ADVANCED

This screen contains advanced SIP configuration settings.

Once settings are configured click **Save/Apply** to begin using the service.

Line 1 & 2	Ports FXS1 & FXS2
Forwarding number	Enter the forwarding phone number
Call forwarding when busy	Tick the checkbox to enable this option
Forwarding all calls	Tick the checkbox to enable this option
Call forwarding if no answer	Tick the checkbox to enable this option
Call waiting (default: enabled)	Tick the checkbox to enable this option

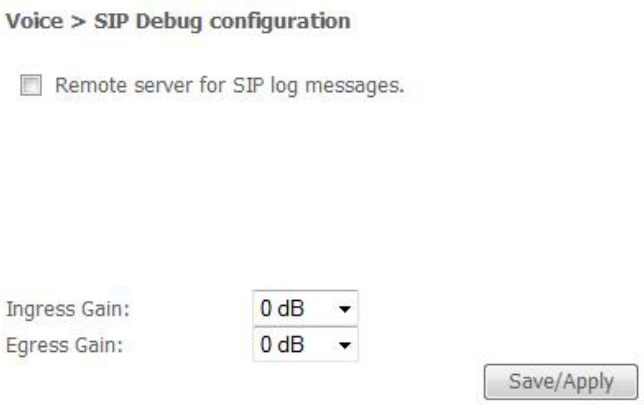
NOTE: These options can also be set using telephone keypad commands, as described in the call command list of section 8.2 Telephone Calls

Enable MWI Subscription	Enable or disable Message-Waiting Indicator (MWI) for FXS Phones with this checkbox.
Enable T.38 support (default: enabled)	Enable or disable T.38 Fax mode support with this checkbox. You can plug a fax machine into either phone port to send or receive faxes. Functionality depends upon FAX support by your VoIP service provider.
Max Digits	Sets the maximum number of digits for a phone number.
Emergency Setting	Multiple emergency numbers can be set using the "|" character (shift + backslash). For example, to set 911 and 114 as emergency numbers, enter "911|114". Please Note: These numbers must be changed to correspond to the emergency numbers that are used in your location.
Dtmf Relay Setting	Set the special use of RTP packets to transmit digit events.
SIP Transport Protocol	Set the special use of SIP protocol to transmit digit events.
Incoming PSTN Call Routing	If PSTN route rule is Auto, an incoming PSTN call will ring an idle phone, either Phone1 or Phone2 (if Phone1 is busy). If PSTN route rule is Line1 or Line2, an incoming PSTN call will attempt to ring only the assigned phone line (FXS1 or FXS2).

Enable SIP tag matching	Select if required by your VoIP provider. (e.g. disable with Vonage service.)
Enable Music Server	Enable/disable the Music Server. Enter the Music Server IP address and port.

5.1.3 SIP DEBUG

This screen contains SIP configuration settings used for debugging.



Once settings are configured click **Save/Apply** to begin using the service.

5.2 Telephone Calls

To make a call, simply dial the number. The dial plan (i.e. the dialled digits) is normally customized for each installation. The default dial plan allows for dialling of 4-digit extensions or direct IP addresses. Shorter extension numbers (e.g. 3-digits) can be dialled by completing the dial string with a final #.

When a Call Server (SIP Proxy Server) is configured into the system, the dialled digits are translated and routed by the Call Server to the correct destination as registered with the Call Server.

If no Call Server is configured, calls can still be made using 4-digit extensions, rather than using full IP addresses. The originator translates the dialled-digits to a destination device as follows:

First Digit:	Line identifier (for multi-line gateways)
Remaining digits:	Host number part of an IP address. The Network number part is considered to be the same as the caller's IP address.

For example, if a caller at address 10.136.64.33/24 dials "2023", the call will be placed to the second line at address 10.136.64.23. All devices have to be on the same Class C subnet (24-bit subnet mask).

To dial an IP address directly, dial the IP address digits using * on the keypad as the dot. Complete the address with a final * or #. When using IP address dialling it is not possible to specify which line at a gateway is called, so the gateway always routes IP-address dialled calls to the first line.

Network busy tone (fast busy) will be played for unknown or unreachable destinations. To answer a call, pick up the phone or press the hands free button.

CALL COMMAND LIST

Caller ID

The Call Manager delivers Caller ID when placing calls. The caller ID is transmitted to the analog line for CLASS recognition.

Call Hold

To put a call on hold, press flash then hang up (optional). To return to the original call, press flash or pick up the phone. The phone will issue a short ring burst every 30 seconds or so while on-hook to remind you that a call is on hold.

Call Transfer

- To transfer a call, press flash then dial the new number.
- To transfer immediately, hang up (blind transfer).
- To transfer with consultation, wait for the party to answer, consult, and hang up.
- To abort the transfer (if the third party does not answer); press flash to return to the original call.

Conference Calling

To turn a two-party call into a three-party conference call, press flash and dial the third party. Wait for the party to answer, then press flash. To drop the third party and return to a two-party call, press flash again. To drop yourself out of the conference, hang up. The call will be transferred (so that the other two parties remain connected to each other).

NOTE: In conference mode, the conference initiator performs the audio bridge/mixing function – there are only two voice streams established.

Call Waiting

If call waiting is enabled on a line, and you hear the call waiting tone during a call, press flash to answer the second call. The first call is automatically placed on hold. To switch between calls, press flash again.

- To disable the call waiting feature, dial *60.
- To enable the call waiting feature, dial *61.

NOTE: Call forward feature settings (Busy or All) take priority over the call-waiting feature. The call-waiting feature is ignored on new incoming calls if there is already a call on hold or in conference.

Call Forward Number

- To set the call forward number, dial *74 then the number. (Note that this does not actually enable forwarding; to do so, select the call forward action as described below.)
- To disable all call forwarding features, dial *70

Call Forward No Answer

- To enable call forward on no answer, dial *71. Incoming calls will be forwarded if unanswered for 18 seconds.

Call Forward Busy

- To enable call forward if busy, dial *72. Incoming calls will forward immediately if the phone is off-hook.

Call Forward All

- To enable call forward for all calls, dial *73.
- To disable the “forward all calls” feature, dial *75. Settings for Call Forward Busy or No Answer are not modified.

Call Return

- To place a call to the last known incoming caller (unanswered or not), dial *69.

Redial

- To redial the last outgoing number, dial *68.

Wireless

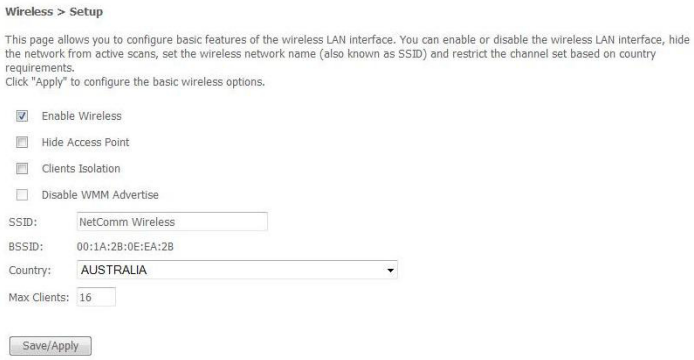
The Home Of All Your Wireless Settings

Wireless

The Wireless dialog box allows you to enable the wireless capability, hide the access point, set the wireless network name and restrict the channel set.

6.1 Setup

The Setup option allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.


Wireless > Setup
This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.
Click "Apply" to configure the basic wireless options.
Enable Wireless
Hide Access Point
Clients Isolation
Disable WMM Advertise
SSID: NetComm Wireless
BSSID: 00:1A:2B:0E:EA:2B
Country: AUSTRALIA
Max Clients: 16
Save/Apply

Click **Save/Apply** to configure the basic wireless options.

Option	Description
Enable Wireless	A checkbox that enables or disables the wireless LAN interface. When selected, the Web UI displays Hide Access point, SSID, and County settings. The default is Enable Wireless.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. If you do not want the access point to be automatically detected by a wireless station, this checkbox should be de-selected. The station will not discover this access point. To connect a station to the available access points, the station must manually add this access point name in its wireless configuration. In Windows XP, go to the Network>Programs function to view all of the available access points. You can also use other software programs such as NetStumbler to view available access points.
Clients Isolation	1. Prevents clients PC from seeing one another in My Network Places or Network Neighborhood.
	2. Prevents one wireless client communicating with another wireless client.
Disable WMM Advertise	Stops the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video). (wireless software version 3.10 and above)
SSID	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access. The naming conventions are: Minimum is one character and maximum number of characters: 32 bytes.
BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Each county listed in the menu enforces specific regulations limiting channel range: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13
Max Clients	The maximum number of clients that can access the router.

6.2 Wireless Security Quick Setup

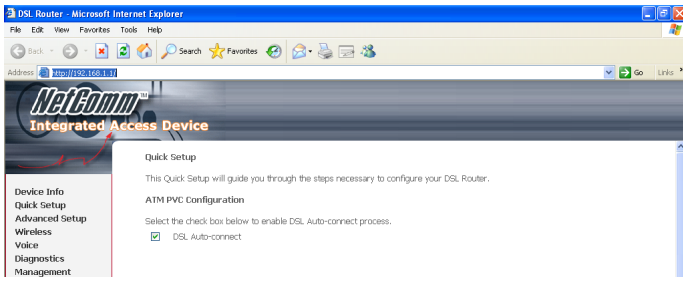
Security settings are used to prevent unauthorised connection to your network. This can be as basic as a neighbouring user who detects and is able to connect through your wireless network, right through to actual malicious interference or 'hacking'. Whatever the case, it is a good practise to be aware of and to use wireless network security to safeguard your data and your network

Prior to considering the details of wireless security – provided later – the Quick Security Setup explains how to implement basic security on your NB9WMAXXn wireless network.

Quick Security Setup 1: WEP Security

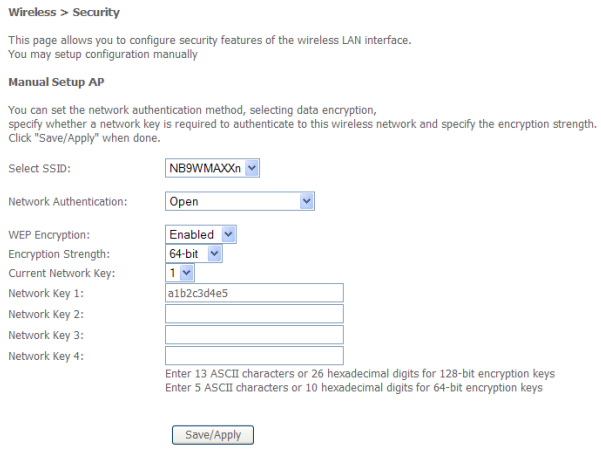
Your NB9WMAXXn has WEP (Wired Equivalent Privacy) encryption enabled by default. Your network will not be available to passer-by or non-authorised users, and any workstation wishing to connect to your NB9WMAXXn must know the SSID (wireless network name) and WEP key values.

Turn on wireless, and set the SSID or wireless network name in the Wireless Setup Screen:



Default SSID: wireless. This can continue to be used or changed to the name of your choice.

Next, click on Wireless>Security. You should see that WEP encryption is enabled by default.


Wireless > Security
This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
Manual Setup AP
You can set the network authentication method, selecting data encryption,
specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Save/Apply" when done.
Select SSID: NB9WMAXXn
Network Authentication: Open
WEP Encryption: Enabled
Encryption Strength: 64-bit
Current Network Key: 1
Network Key 1: a1b2c3d4e5
Network Key 2:
Network Key 3:
Network Key 4:
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys
Save/Apply

This page will also allow you to change the Network Authentication and encryption key.

Default WEP Key: a1b2c3d4e5

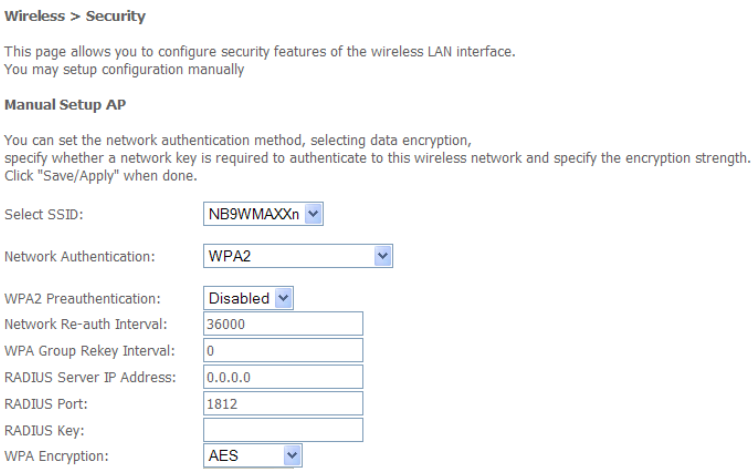
You are able to change these values however it is strongly recommended that security is not turned off. It is also recommended that your SSID or network name not advertise your actual name but be kept 'generic' or anonymous.

Note: WEP Security is the appropriate choice if the network clients that wish to connect include 802.11b standard NICs.

Quick Security Setup 2 – WPA-PSK

If a stronger network security settings is required, go to Wireless>Security and select WPA-PSK from the Network Authentication drop-down menu. Enter a network key of your choice in the WPA Pre-Shared Key field; this can be from 8 to 63 characters and contain special characters and spaced. And change the WPA Group Rekey Interval to 3600.

Select TKIP for WPA Encryption and leave WEP Encryption as disabled.



Users wishing to connect to your network will need to know the SSID name and the WPA Pre-Shared Key.

Note: Wireless client network cards must be WPA-compliant to connect to your network; if in doubt check the wireless client network card documentation, or use WEP security (above).

6.3 Wireless Security in Detail

The following provides a detailed summary of wireless terms and acronyms and more in-depth explanations of the topic. It assumes little prior knowledge of wireless networking and is aimed at providing background for the terminology used in the NB9WMAXXn Wireless Security screens.

Warning: Wireless Networking is a technically challenging subject!

Authentication and Encryption

The two major aims of wireless network security are:

(1) to prevent unauthorised persons from joining the network and

(2) to prevent interception of network data or 'eavesdropping'. These aims are accomplished by:

- Authentication: establishes the identity of those seeking to join the network
- Encryption: ensures that data is protected in such a way that those outside the network cannot access it.

Network Keys

The term 'network key' is often used in the context of wireless networking. The Network Key can be a text string, although in some systems network keys are generated from a 'pass-phrase' which is entered in one field from which up to four keys are derived in fields underneath the entry field.

In all cases, the Wireless Router/Access Point and the workstations wishing to connect must use the same Network Key which needs to be communicated to clients prior to connection.

'Re-keying' refers to the frequency with which network keys are changed; for security purposes, they need to be changed frequently in case they re-occur frequently enough to identify them.

In some wireless systems, network keys are entered by a variety of means including:

- ASCII – any letter, number, or punctuation mark but no special characters
- Hex – Letters A-F, Numbers 0-9 only
- Pass phrase – enter a phrase in the top field of a set of fields, an algorithm then generates a series of keys based on the entered values.

These methods have been standardised in the later implementations of Wireless Security and are easier to use in WPA.

WEP and WPA

"WEP" stands for Wired Equivalent Privacy and was the original wireless security method. Over time it was found to be vulnerable to attacks based on de-coding the 'keys' used to encrypt the data. While no longer recommended for enterprise-level security, WEP is certainly secure from casual interception and will repel any non-specialised attempt to join the network or intercept data; it can be penetrated with various kinds of software tools and techniques but these are beyond the capability of the average computer user.

'WPA' stands for Wi-Fi Protected Access and is an improvement on WEP. WPA2 offers further refinements to WPA.

WPA and WPA2 both comprise a number of different wireless security elements and methods that can be adapted to a variety of situations depending on the requirements. A lot of what is provided is applicable to enterprise-level wireless networking, in other words, suitable for businesses who wish to deploy strict security methods and policies for their employees. Accordingly, these technologies will exceed the requirements of home users.

An important element of WPA security is a RADIUS server (stands for Remote Access Dial-in User Service). The RADIUS server typically sits in the server room of a business or department and authenticates and manages user requests for connection. Home users will generally never have to bother about RADIUS server details.

In nearly all cases, the default security method, which is WEP, or WPA-PSK will provide adequate security for home wireless networks.

Other wireless security elements shall be explained in context below.

Network Authentication

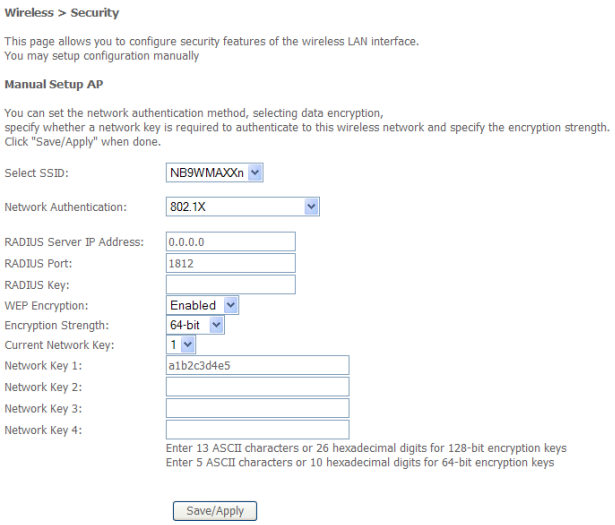
Network Authentication specifies the type of network authentication. The default value is 'Shared'.

Open:	Under Open System authentication, any wireless station can request authentication.
Shared:	Under Shared Key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel (i.e. verbally). To use Shared Key authentication, you must have a network key assigned to the clients trying to connect to your NB9WMAXXn.

802.1X

802.1X security requires the presence of a RADIUS server, and specification of the IP address of a RADIUS server, the port on which to connect to it, and the Shared Key used to authenticate with it.

Disregard this security setting unless you are setting up or connecting to a RADIUS server.


Wireless > Security
This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
Manual Setup AP
You can set the network authentication method, selecting data encryption,
specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Save/Apply" when done.
Select SSID:
NB9WMAXXn
Network Authentication:
802.1X
RADIUS Server IP Address:
0.0.0.0
RADIUS Port:
1812
RADIUS Key:
WEP Encryption:
Enabled
Encryption Strength:
64-bit
Current Network Key:
1
Network Key 1:
a1b2c3d4e5
Network Key 2:
Network Key 3:
Network Key 4:
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys
Save/Apply

WPA

WPA requires a RADIUS server to provide client authentication. WPA also requires specification of the 'WPA Group Rekey Interval' which is the rate that the RADIUS server sends a new Group Key out to all clients. The Re-Keying process is part of WPA's enhanced security. This method also requires specification of the IP address of a RADIUS server, the port on which to connect to the RADIUS server, and the shared key used to authenticate with the RADIUS server.

WPA-PSK

WPA-PSK is a special mode of WPA providing strong encryption without access to a RADIUS server.

In this mode encryption keys are automatically changed (rekeyed) and authentication re-established between devices after a specified period referred to as the 'WPA Group Rekey Interval'.

WPA-PSK is far superior to WEP and provides stronger protection for the home/SOHO user for two reasons: first, the process used to generate the encryption key is very rigorous and second, the rekeying (or key changing) is done very quickly. This stops even the most determined hacker from gathering enough data to identify the key and so break the encryption.

WEP is confusing because of the various types of 'network keys' vendors use (HEX, ASCII, or passphrase) and because home users mix and match equipment from multiple vendors, all using different types of keys. But WPA-PSK employs a consistent, easy to use method to secure your network. This method uses a passphrase (also called a shared secret) that must be entered in both the NB9WMAXXn and the wireless clients. This shared secret can be between 8 and 63 characters and can include special characters and spaces. For maximum security, the "WPA Pre-Shared Key" should be a random sequence of either keyboard characters (upper and lowercase letters, numbers, and punctuation) at least 20 characters long, or hexadecimal digits (numbers 0-9 and letters A-F) at least 24 hexadecimal digits long.

Note: The less obvious, longer and more 'random' your 'WPA Pre-Shared Key', the more secure your network.

Note the following 'WPA Encryption' options:

TKIP:	The Temporal Key Integrity Protocol (TKIP) takes over after the initial shared secret is entered in your wireless devices and handles the encryption and automatic rekeying.
AES:	WPA defines the use of Advanced Encryption Standard (AES) as an additional replacement for WEP encryption. Because you may not be able to add AES support through a firmware update to your existing wireless clients / equipment, support for AES is optional and is dependent on vendor driver support.
TKIP+AES:	This will allow either TKIP or AES wireless clients to connect to your NB9WMAXXn.

WPA2

'WPA Pre-authentication' support in WPA2 allows a client to pre-authenticate with the NB9WMAXXn toward which it is moving, while maintaining a connection to the access point it's moving away from. This new capability allows the roaming to occur in less than 1/10th of a second while a traditional roam without PMK caching and pre-authentication would take more than one second. Time-sensitive applications like Citrix, video, or VoIP will all break without fast roaming.

'Network Re-Auth Interval' is the interval specified (seconds) that the wireless client needs to re-authenticate with the NB9WMAXXn.

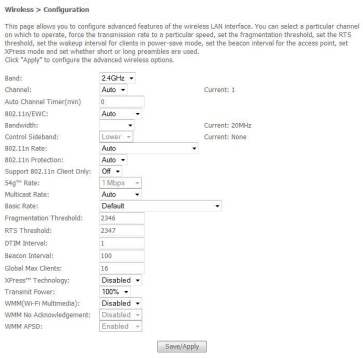
For the remainder of the fields required, see above.

WPA2-PSK:	Same as WPA-PSK, but you can only use AES with WPA2 and not WPA.
Mixed WPA2/WPA:	Enables WPA2 or WPA wireless clients to connect to the NB9WMAXXn. Requires a RADIUS server to authenticate the wireless clients.
Mixed WPA2/WPA-PSK:	Enables WPA2 and WPA clients to authenticate using a PSK (Pre-Shared Key) instead of a RADIUS server.

6.4 Configuration

The Configuration screen allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

Click **Apply** to configure the advanced wireless options.


Wireless > Configuration
This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.
Click "Apply" to configure the advanced wireless options.
Band:
Channel:
Auto Channel Timer(min)
802.11n/EWC:
Bandwidth:
Control Sideband:
802.11n Rate:
802.11n Protection:
Support 802.11n Client Only:
54g™ Rate:
Multicast Rate:
Basic Rate:
Fragmentation Threshold:
RTS Threshold:
DTIM Interval:
Beacon Interval:
Global Max Clients:
XPress™ Technology:
Transmit Power:
WMM(Wi-Fi Multimedia):
WMM No Acknowledgement:
WMM APSD:
Save/Apply

Option	Description
Band	Frequency band used by the wireless AP. Default is 2.4GHz
Channel	Drop-down menu that allows selection of a specific channel.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
802.11n/EWC	With drop-down menu, “Auto” is for 11n and “Disable” is for 11g
Bandwidth	Drop-down menu specifies the following bandwidth: 20MHz in 2.4G Band and 40 MHz in 5G Band, 20MHz in both bands and 40MHz in both bands
Control Sideband	This is available for 40MHz. Drop-down menu allows selecting upper sideband or lower sideband
802.11n Rate	Drop-down menu specifies the following fixed rates. The maximum rate for bandwidth, 20MHz, is 130MHz and the maximum bandwidth, 40MHz, is 270MHz
802.11n Protection	It is similar as 802.11g protection. In Auto mode the router will use RTS/CTS to improve 802.11n performance in mixed 802.11n/ 802.11g/ 802.11b networks. Turn protection off to maximize 802.11n throughput under most conditions.
Support 802.11n client only	Drop-down menu allows selecting “On/Off”. Choosing “On” allows the client with 11n only to connect, not for 11g or 11b; choosing “Off” allows the client with 11n/11g/11b to connect
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting multicast packet transmit rate.
Basic Rate	Setting basic transmit rate.
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM), also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions. Each beacon transmission identifies the presence of an access point. By default, radio NICs passively scan all RF channels and listen for beacons coming from access points to find a suitable access point. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point). The entered value is represented in ms. Default is 100. Acceptable entry range is 1 to 0xffff (65535)
Global Max Clients	The device can support 4 SSID, and each SSID can set its own max clients, but it can’t be bigger than Global max clients. “Global Max Clients” limits the total associated clients of the 4 SSID.
Xpress TM Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.

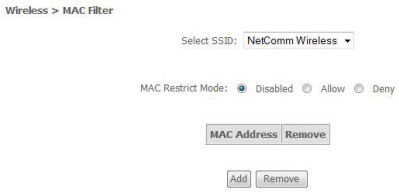
Transmit Power	The router will set different power output (by percentage) according to this selection.
WMM (Wi-Fi Multimedia)	The technology maintains the priority of audio, video and voice applications in a Wi-Fi network. It allows multimedia service get higher priority.
WMM No Acknowledgement	Refers to the acknowledge policy used at the MAC level. Enabling no Acknowledgement can result in more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.
WMM APSD	This is Automatic Power Save Delivery. It saves power.

6.5 MAC Filter

This option allows access to the router to be restricted based upon MAC addresses. Every network device has a unique 48-bit MAC address. This is usually shown as xx.xx.xx.xx.xx.xx, where xx are hexadecimal numbers. When MAC address filtering is enabled, it restricts the devices that can connect to your access point.

To add a MAC Address filter, click the **Add** button shown below.

To delete a filter, select it from the table below and click the **Remove** button.



Option	Description
MAC Restrict Mode	Disabled: MAC filtering function is disabled. Allow: Permits PCs with listed MAC addresses to connect to access point. Deny: Prevents PCs with listed MAC from connecting to the access point.
MAC Address	Lists the MAC addresses subject to the MAC Restrict Mode. A maximum of 60 MAC addresses can be added. Every network device has a unique 48-bit MAC address. This is usually shown as xx.xx.xx.xx.xx.xx, where xx are hexadecimal numbers.

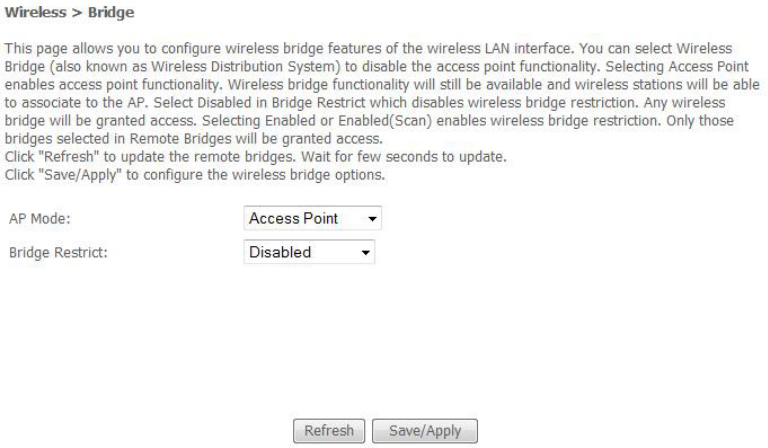
After clicking the **Add** button, the following screen appears.

Enter the MAC address in the box provided and click **Save/Apply**.

Wireless > MAC Filter
Enter the MAC address and click "Apply" to add the MAC address to the wireless MAC address filters.
MAC Address:
Save/Apply

6.6 Wireless Bridge

This screen allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict, which disables wireless bridge restriction. Any wireless bridge will be granted access. Select **Enabled** or **Enabled (Scan)** to enable the wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.


Wireless > Bridge
This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable the access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.
Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Save/Apply" to configure the wireless bridge options.
AP Mode:
Access Point
Bridge Restrict:
Disabled
Refresh
Save/Apply

6.7 Station Info

This screen shows authenticated wireless stations and their status.

Management

Control And Administer Your Device

Management

7.1 Device Settings

The Device Settings option allows you to back up your settings to a file, retrieve the setting file, and restore the settings.

7.1.1 Backup

The Backup option under Management > Device Settings saves your router configurations to a file on your PC. Click Backup Settings in the main menu. You will be prompted to define the location of the backup file to save. After choosing the file location, click Backup Settings. The file will then be saved to the assigned location.

Management > Device Settings > Backup
Backup DSL router configurations. You may save your router configurations to a file on your PC.
Backup Settings

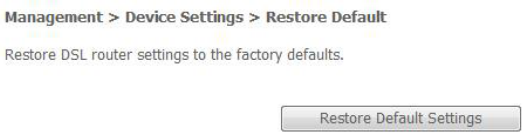
7.1.2 Update

This option updates your router settings using a previously saved settings file.

Management > Device Settings > Update
Update DSL router settings. You may update your router settings using your saved files.
Settings File Name:
Browse...
Update Settings

7.1.3 Restore Default

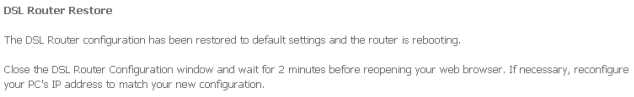
Clicking the Restore Default Configuration option in the Restore Settings screen can restore the original factory installed settings (see section 3.3 Default Settings).


Management > Device Settings > Restore Default
Restore DSL router settings to the factory defaults.
Restore Default Settings

NOTE 1: This option has the same effect as the hardware reset-to-default button on the rear panel of the router. The device board hardware and the boot loader support the reset to default button. If the reset button is pressed for more than 10 seconds, the configuration data will be erased.

NOTE 2: Restoring system settings requires a system reboot. The current Web UI session must be closed and restarted. Before restarting it, the IP configuration may need to be configured with a static IP address.

After the Restore Default Configuration button is selected, the following screen appears. Close the window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC IP address to match your new configuration.


DSL Router Restore
The DSL Router configuration has been restored to default settings and the router is rebooting.
Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

7.1.4 Update Firmware

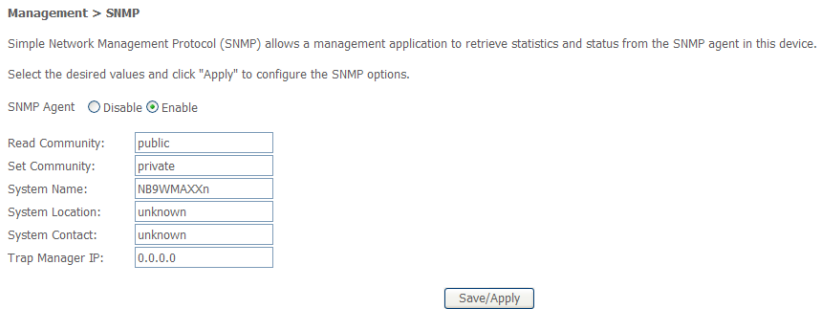
The Update firmware screen allows you to update the firmware of the device. Manual firmware upgrades from a locally stored file can be performed using the following screen. Your ISP will provide this file to you, if necessary.

Mangement > Setting > Update Firmware
Step 1: Obtain an updated software image file from your ISP.
Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
Step 3: Click the "Update Software" button once to upload the new image file.
NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.
Software File Name:
Browse...
Update Software

7.2 SNMP

The Simple Network Management Protocol (SNMP) allows a network administrator to monitor a network by retrieving settings on remote network devices. To do this, the administrator typically runs an SNMP management station program such as MIB browser on a local host to obtain information from the SNMP agent, in this case the NB9WMAXXn (if SNMP enabled). An SNMP 'community' performs the function of authenticating SNMP traffic. A 'community name' acts as a password that is typically shared among SNMP agents and managers.

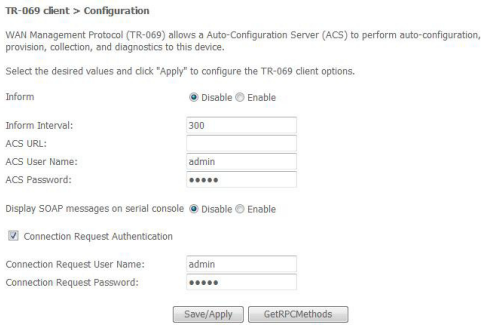
To enable SNMP, change the setting for "SNMP Agent" to "Enable".



Field	Means
Read Community	Read device settings.
Set Community	Read and change device settings.
System Name	Default = NB9WMAXXn.
System Location	User-defined value.
System Contact	User-defined value.
Trap Manager IP	IP Address of admin machine.

7.3 TR-069 Client

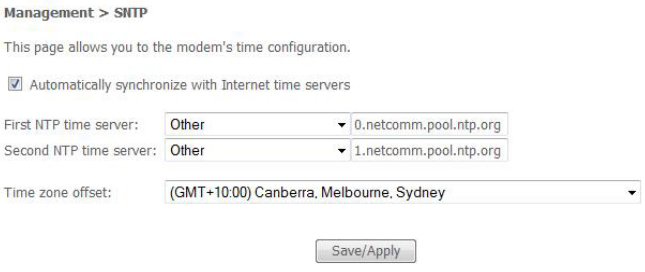
WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this router.



Option	Description
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
Connection Request Authentication	Enable/Disable authentication of ACS making a Connection Request to the CPE.
Connection Request User Name	Username used to authenticate an ACS making a Connection Request to the CPE.
Connection Request Password	Password used to authenticate an ACS making a Connection Request to the CPE.
Get RPC Methods	This method may be used by a CPE or ACS to discover the set of methods supported by the ACS or CPE it is in communication with. This list may include both standard TR-069 methods (those defined in this specification or a subsequent version) and vendor-specific methods. The receiver of the response MUST ignore any unrecognized methods. Click this button to force the CPE to establish an immediate connection to the ACS.

7.4 SNTP

The Internet Time option under the Management submenu configures the time settings of the device. To automatically synchronize with Internet time servers, tick the corresponding box displayed on this screen shown below.



First NTP time server: Select the required server.

Second NTP time server: Select second time server, if required.

Time zone offset: Select the local time zone.

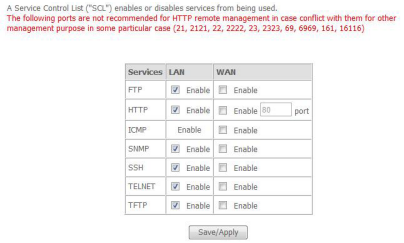
Configure these options and then click Save/Apply to activate.

7.5 Access Control

The Access Control option under the Management menu configures three access-related parameters: Services, IP Address and Passwords.

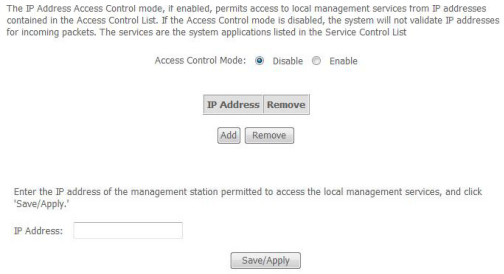
7.5.1 Services

The Services option limits or opens the access services over the LAN or WAN. These services are provided FTP, HTTP, ICMP,SNMP, SSH (Security Socket Share), TELNET, and TFTP. Enable the service by checking the item in the corresponding checkbox, and then click **Save/Apply**.



7.5.2 Access IP Addresses

The IP Addresses option limits access by IP address. If Access Control Mode is enabled, only the IP addresses listed here can access the router. Before enabling it, configure the IP addresses by clicking the **Add** button. Enter the IP address and click **Apply** to allow the PC with this IP address to manage the device.

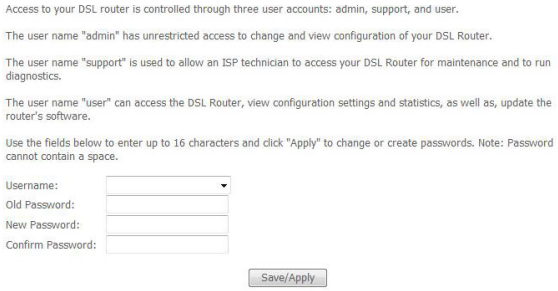

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List
Access Control Mode:
Disable
Enable
IP Address
Remove
Add
Remove
Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'
IP Address:
Save/Apply

7.5.3 Passwords

The Passwords option configures the access passwords for the router. Access to your router is controlled through three user accounts: root, support, and user.

- root has unrestricted access to change and view the configuration of your router. It is the top administrative account.
- support is intended to allow limited access so that a technical support representative can conduct maintenance and run diagnostics.
- user provides the least access control but allows for viewing configuration settings and statistics, as well as, updating software.

Use the fields below to enter up to 16 characters and click Save/Apply to change or create passwords. See section 3.3 Default Settings for the default passwords.


Access to your DSL router is controlled through three user accounts: admin, support, and user.
The user name "admin" has unrestricted access to change and view configuration of your DSL Router.
The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.
The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.
Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.
Username:
Old Password:
New Password:
Confirm Password:
Save/Apply

7.6 Save and Reboot

The Save/Reboot button saves the configurations and reboots the router. After clicking it, wait for 2 minutes before attempting to use the user interface. You may need to close and restart the web browser if it does not refresh automatically. You may need to reconfigure your PC IP address to match your new configuration. In this case, see section 3.1 Configuring your computer for detailed instructions.

Advanced

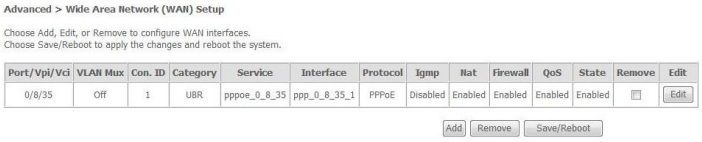
High Level Configuration Options

Advanced

This chapter explains the Advanced Setup menu options outlined below.

8.1 WAN

This screen allows for the advanced configuration of WAN interfaces.


Advanced > Wide Area Network (WAN) Setup
Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Save/Reboot to apply the changes and reboot the system.
Port/Vpi/Vci VLAN Mux Con. ID Category Service Interface Protocol Igmp Nat Firewall QoS State Remove Edit
0/8/35 Off 1 UBR pppoe_0_8_35 ppp_0_8_35_1 PPPoE Disabled Enabled Enabled Enabled Enabled Edit
Add Remove Save/Reboot

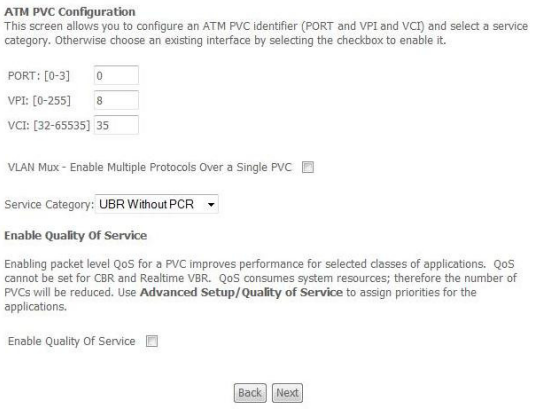
- To Add a WAN connection, click the **Add** button. To edit an existing connection, click the Edit button next to the connection. To complete the Add or Edit, on the opening screen, select VLAN Mux (see section 9.1.1VLAN Mux) and then proceed to STEP 2 in section 4.2 Manual Quick Setup.
- To remove a connection select its radio button under the Remove column in the table and click the **Remove** button under the table.
- **Save/Reboot** activates the new configuration.

Field	Description
Port/VPI/VCI	ATM Port (0-3) / VPI (0-255) / VCI (32-65535)
VLAN Mux	Shows 802.1Q VLAN ID
Con. ID	ID for WAN connection
Category	ATM service category, e.g. UBR, CBR…
Service	Name of the WAN connection
Interface	Name of the interface for WAN
Protocol	Shows bridge or router mode
IGMP	Shows enable or disable IGMP proxy
NAT	Enable/Disable NAT (Leave enabled unless advised otherwise by tech support)
Firewall	Enable/Disable Firewall (Leave enabled unless advised otherwise by tech support)
QoS	Shows enable or disable QoS
State	Shows enable or disable WAN connection

8.1.1 VLAN Mux

VLAN Mux is a form of VLAN tagging that allows multiple protocols over a single connection.

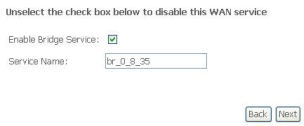
Adding a new connection with VLAN Mux is accomplished by selecting the VLAN Mux – Enable Multiple Protocols Over a Single PVC check box (as outlined in red below). Enter a value for 802.Q VLAN ID in the box that appears below.


ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (PORT and VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.
PORT: [0-3] 0
VPI: [0-255] 8
VCI: [32-65535] 35
VLAN Mux - Enable Multiple Protocols Over a Single PVC
Service Category: UBR Without PCR
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service
Back Next

After proceeding to STEP 3 in section 4.2 Manual Quick Setup, the screen will appear as follows. Notice that PPPoA and IPoA are not available.

PVCs can be added using the regular procedure, however, now multiple protocols can exist over the same connection, as long as the 802.1Q VLAN IDs differ.

The graphic below shows an example of three protocols over the same connection.



8.1.2 MSP

Multi-Service over PVC (MSP) supports multiple protocols over a single connection. As with the VLAN Mux function, PPPoE, Bridge and MER protocols can coexist, while IPoA and PPPoA are not supported. This function supports remote management by bridge protocol in addition to multimedia applications over a single PVC.

Configuring MSP is a two-part process:

Part 1 - Create multiple PVCs (One Bridge + multiple PPPoE / One MER)

Part 2 - Use Port Mapping to connect LAN / WAN interfaces

NOTE: The example below shows how to configure a Bridge / PPPoE MSP connection. Use the same process for Bridge / MER MSP connections.

If QoS is configured on the first MSP connection, it will be configured by default for all subsequent connections.

If a MSP connection is removed every other MSP connection should be removed to avoid port mapping configuration problems.

Part 1 – Create Multiple PVCs

On the Advanced – WAN screen, create one PPPoE connection and one Bridge connection on the MSP supporting PVC. The screen will display as follows.

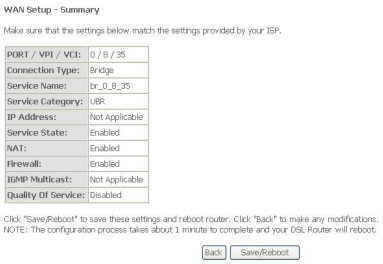
Part 2

Go to Advanced – Port Mapping screen (see section 9.9 Port Mapping) and select the Enable Virtual Ports checkbox. The screen will display as follows.

NOTE: Only hardware ports and bridge PVCs are listed as interfaces. The bridge interface is shown as “nas_x_y_z” where x=port, y=vpi, and z=vci.

To continue, click the **Add** button at the bottom of the screen shown above.

On the screen shown below, select the bridge connection and one Ethernet virtual port (ENET 1-4). Enter a group name, such as “MSP1”, and click **Save/Apply**.



WAN Setup - Summary

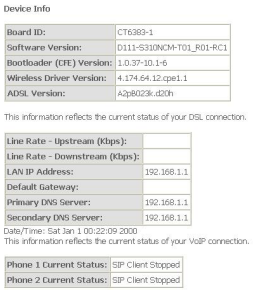
Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 8 / 35
Connection Type:	Bridge
Service Name:	br_0_8_35
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

Back Save/Reboot

If successfully configured, the Port Mapping screen will display as follows.



Device Info

Board ID:	CT6383-1
Software Version:	D111-S310NCM-T01_R01-RC1
Bootloader (CFE) Version:	1.0.37-10.1-6
Wireless Driver Version:	4.174.64.12.cpe1.1
ADSL Version:	A2pB023k.d20h

This information reflects the current status of your DSL connection.

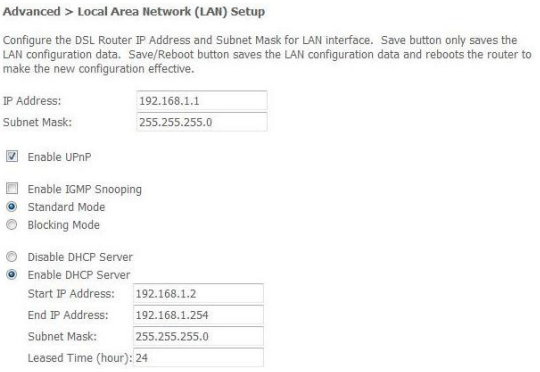
Line Rate - Upstream (Kbps):	
Line Rate - Downstream (Kbps):	
LAN IP Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	192.168.1.1
Secondary DNS Server:	192.168.1.1

Date/Time: Sat Jan 1 00:22:09 2000
This information reflects the current status of your VoIP connection.

Phone 1 Current Status:	SIP Client Stopped
Phone 2 Current Status:	SIP Client Stopped

8.2 LAN

Use this screen to configure LAN interface settings.


Advanced > Local Area Network (LAN) Setup
Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Enable UPnP
Enable IGMP Snooping
Standard Mode
Blocking Mode
Disable DHCP Server
Enable DHCP Server
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0
Leased Time (hour): 24

NOTE: NAT is enabled so Enable UPnP is shown above while DHCP Server Relay is hidden. Consult the field descriptions below for more details.

Field	Means
LAN IP Address	Default: 192.168.1.1. The LAN IP address of your NB9WMAXXn.
LAN Subnet Mask	Default: 255.255.255.0. The subnet mask of your NB9WMAXXn. A subnet mask is used to determine what subnet an IP address belongs to. For more information on subnetting see http://www.ralphb.net/IPSubnet/.
Enable UPnP	Universal plug and play (UPnP) allows traffic to pass through the NB9WMAXXn for applications using the UPnP protocol. This feature requires one active WAN connection. In addition, the client connecting to the NB9WMAXXn should support this feature. UPnP also supports NAT Traversal which can automatically solve many NAT-related communications problems. UPnP enables applications to assign dynamic port mappings to the NB9WMAXXn and delete them when connections are complete. A typical example is the MSN Messenger application that runs on Windows. Instead of manually setting up the port mappings UPnP enables MSN Messenger to make the request to the NB9WMAXXn which will setup these ports dynamically. When MSN Messenger is closed the port openings will be removed from the NB9WMAXXn's configuration. Configure the second IP address and subnet mask for LAN interface. It is possible to configure the second IP address to access the NB9WMAXXn on. Once this box is checked you are able to enter the IP address and subnet mask.
Disable DHCP Server	Disables the DHCP server. Only to be done if Static IP address is set up.
Enable DHCP Server	Default: Enabled.
Start IP Address	Default: 192.168.1.2. The first IP address that will be issued to the first DHCP client connecting to the NB9WMAXXn using Ethernet cable or wirelessly.
End IP Address	Default: 192.168.1.254. The last IP address in the DHCP pool to be issued to DHCP clients connecting to the NB9WMAXXn.
Lease Time	Default: 24 hours. The time an IP address is assigned to a client before being renewed.
Enable IGMP Snooping	IGMP specifies how a host can register a router in order to receive specific multicast traffic. IGMP Snooping allows the NB9WMAXXn to capture IGMP frames. When your NB9WMAXXn hears an IGMP report from a host for a given multicast group it adds the host's port number for that group. When the NB9WMAXXn hears an IGMP Leave, it removes the host's port from the table entry. Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group. IGMP Snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your NB9WMAXXn.
Save	Save the settings.
Save / Reboot	Save and reboot with the settings applied.

NOTE: The Save button saves new settings to allow continued configuration while the Save/Reboot button not only saves new settings but also reboots the device to apply the new configuration (i.e. all new settings).

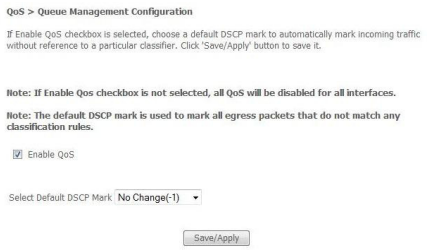
8.3 QoS Classification

Quality of Service (QoS) can provide different priority to different users or data flows, or guarantee a certain level of performance to a data flow in accordance with requests from Queue Prioritization.

NOTE: QoS must be enabled in at least one PVC to display this option. (see Advanced Setup - WAN for detailed PVC setup instructions).

8.3.1 Queue Management Configuration

To Enable QoS tick the checkbox, select Default DSCP Mark and click **Save/Apply**.

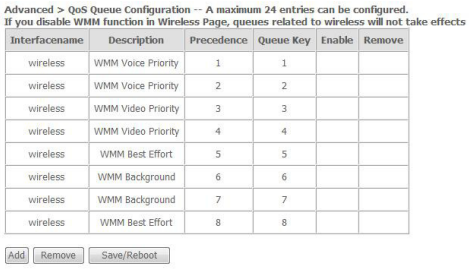

QoS > Queue Management Configuration
If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Save/Apply' button to save it.
Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.
Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.
Enable QoS
Select Default DSCP Mark
No Change(-1)
Save/Apply

Select Default Differentiated Services Code Point (DSCP) Mark

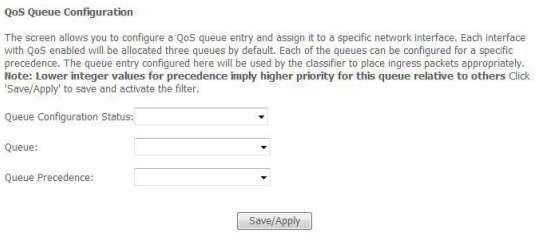
With this drop-down box you can assign a DSCP mark in the Internet Protocol (IP) header that specifies the per hop behavior for a given flow of incoming packets that do not match any other QoS rule.

8.3.2 Queue Configuration

This function follows the **Differentiated Services** rule of IP QoS. You can create a new Queue rule by assigning an Interface, Enable/ Disable and Precedence. The router uses various queuing strategies to tailor performance to user requirements

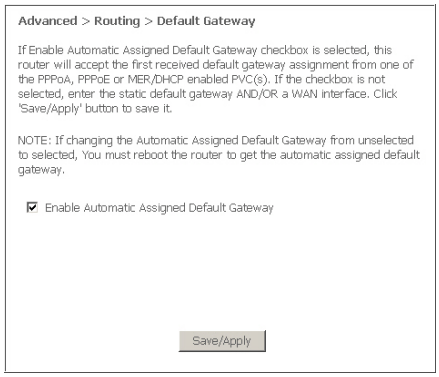

Advanced > QoS Queue Configuration -- A maximum 24 entries can be configured.
If you disable WMM function in Wireless Page, queues related to wireless will not take effects
Interfacename
Description
Precedence
Queue Key
Enable
Remove
wireless WMM Voice Priority 1 1
wireless WMM Voice Priority 2 2
wireless WMM Video Priority 3 3
wireless WMM Video Priority 4 4
wireless WMM Best Effort 5 5
wireless WMM Background 6 6
wireless WMM Background 7 7
wireless WMM Best Effort 8 8
Add
Remove
Save/Reboot

Click **Add** to display the following screen.

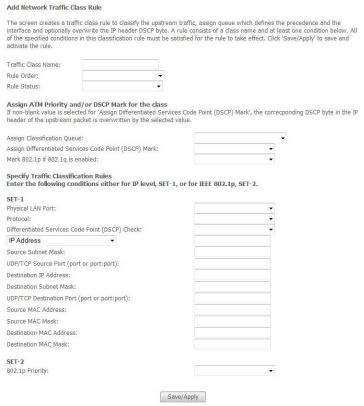

QoS Queue Configuration
The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each interface with QoS enabled will be allocated three queues by default. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately.
Note: Lower integer values for precedence imply higher priority for this queue relative to others Click 'Save/Apply' to save and activate the filter.
Queue Configuration Status:
Queue:
Queue Precedence:
Save/Apply

Field Name	Comment
Queue Configuration Status:	Enable or Disable the queue.
Queue:	Assign queue to a specific network interface whose QoS is enabled.
Queue Precedence:	Configure precedence for the queue. Lower integer values for precedence imply higher priority for this queue relative to others.

8.3.3 QoS Classification


Advanced > Routing > Default Gateway
If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.
NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.
Enable Automatic Assigned Default Gateway
Save/Apply

Click **Add** to configure network traffic classes.



This screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

Click **Save/Apply** to save and activate the rule.

8.4 Routing

8.4.1 Default Gateway

If the **Enable Automatic Assigned Default Gateway** checkbox is selected, this router will accept the first received default gateway assignment from the DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway and/or WAN interface. Click **Save/Apply**.

Advanced > Routing > Default Gateway
If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.
NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.
Enable Automatic Assigned Default Gateway
Save/Apply

NOTE: After enabling Automatic Assigned Default Gateway, you must click the Save/Apply button to put it into effect. The router will reboot.

8.4.2 Static Route

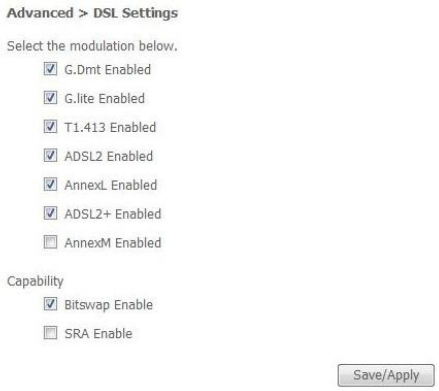
This screen lists the configured static routes and allows for the configuration of static routes. Choose Add or Remove to configure the static routes.

To add static route, click the **Add** button to display the following screen. Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click **Save/Apply** to add the entry to the routing table.

Routing -- Static Route Add
Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Save/Apply" to add the entry to the routing table.
Destination Network Address:
Subnet Mask:
Use Gateway IP Address
Use Interface
pppoe_0_8_35/ppp_0_8_35_1
Save/Apply

8.5 DSL

This screen is used to select ADSL modulations and capabilities.



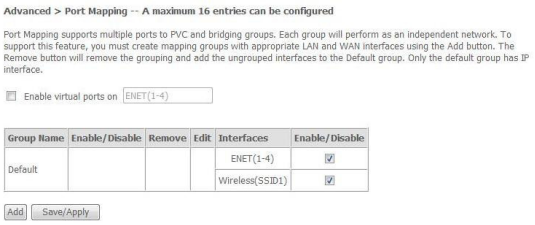
The following table describes these DSL settings

Option	Description
G.dmt	Sets G.Dmt if you want the system to use G.Dmt mode.
G.Lite	Sets G.Lite if you want the system to use G.Lite mode.
T1.413	Sets the T1.413 if you want the system to use T1.413 mode.
ADSL2	The router can support the functions of ADSL2.
AnnexL	The router can support/enhance the long loop test.
ADSL2+	The router can support the functions of ADSL2+.
AnnexM	Enables a higher “upstream” data rate, by making use of some downstream channels.
Inner Pair	Reserved only
Outer Pair	Reserved only
Bitswap Enable	Allows bitswapping function
SRA Enable	Allows seamless rate adaptation

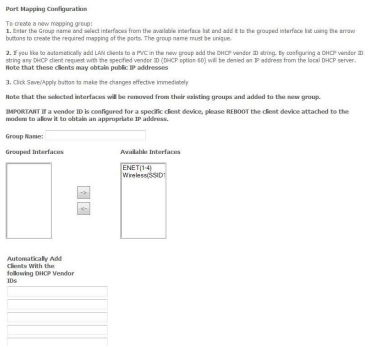
8.6 Port Mapping

Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group.

As shown below, when you tick the Enable virtual ports on checkbox, all of the LAN interfaces will be put together as a default group.


Advanced > Port Mapping -- A maximum 16 entries can be configured
Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.
Enable virtual ports on
ENET(1-4)
Group Name
Enable/Disable
Remove
Edit
Interfaces
Enable/Disable
Default
ENET(1-4)
Wireless(SSID1)
Add
Save/Apply

To add a port mapping group, click the **Add** button.



To create a group from the list, first enter the group name and then select from the available interfaces on the list with the arrow buttons .

Automatically Add Clients With the Following DHCP Vendor IDs:

Add support to automatically map LAN interfaces including Wireless and USB to PVC's using DHCP vendor ID (option 60). The local DHCP server will decline and send the requests to a remote DHCP server by mapping the appropriate LAN interface. This will be turned on when PortMapping is enabled.

There are 4 PVCs (0/33, 0/36, 0/37, 0/38). VPI/VCI=0/33 is for PPPoE and the others are for IP set-top box (video). The LAN interfaces are ENET1, ENET2, ENET3, ENET4, Wireless and USB. Port mapping configuration is:

1. Default: ENET1, ENET2, ENET3, ENET4, Wireless and USB.
2. Video: nas_0_36, nas_0_37 and nas_0_38. The DHCP vendor ID is "Video".

The CPE deco server is running on "Default". And ISP's deco server is running on PVC 0/36. It is for set-top box use only.

On the LAN side, the PC can get IP address from CPE deco server and access the Internet via PPPoE (0/33).

If the set-top box was connected with interface "ENET1" and send a deco request with vendor id "Video", the CPE deco server would forward this request to ISP's deco server. Then the CPE will change the PortMapping configuration automatically.

The PortMapping configuration would become:

1. Default: ENET1, ENET2, ENET3, ENET4, Wireless and USB.
2. Video: nas_0_36, nas_0_37 and nas_0_38 and ENET1.

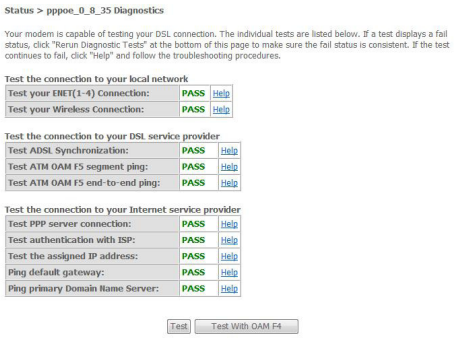
Status

An Overview Of Your Product Settings

Status

9.1 Diagnostics

The Diagnostics menu provides feedback on the connection status of the router and the DSL link. The individual tests are listed below. If a test displays a fail status, click Test at the bottom of this screen to make sure the fail status is consistent. If the test continues to fail, click Help and follow the troubleshooting procedures provided onscreen.


Status > pppoe_0_8_35 Diagnostics
Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.
Test the connection to your local network
Test your ENET(1-4) Connection: PASS Help
Test your Wireless Connection: PASS Help
Test the connection to your DSL service provider
Test ADSL Synchronization: PASS Help
Test ATM OAM F5 segment ping: PASS Help
Test ATM OAM F5 end-to-end ping: PASS Help
Test the connection to your Internet service provider
Test PPP server connection: PASS Help
Test authentication with ISP: PASS Help
Test the assigned IP address: PASS Help
Ping default gateway: PASS Help
Ping primary Domain Name Server: PASS Help
Test
Test With OAM F4

Test	Description
Ethernet Connection	Pass: Indicates that the Ethernet interface from your computer is connected to the LAN port of your router. Fail: Indicates that the router does not detect the Ethernet interface on your computer.
Wireless Connection	Pass: Indicates that the Wireless interface from your computer is connected to the wireless network. Down: Indicates that the router does not detect the wireless network.
ADSL Synchronization	Pass: Indicates that the router has detected an ADSL signal from the telephone company. Fail: Indicates that the router does not detect a signal from the telephone company's DSL network.

Additional tests are added here based upon connection type.

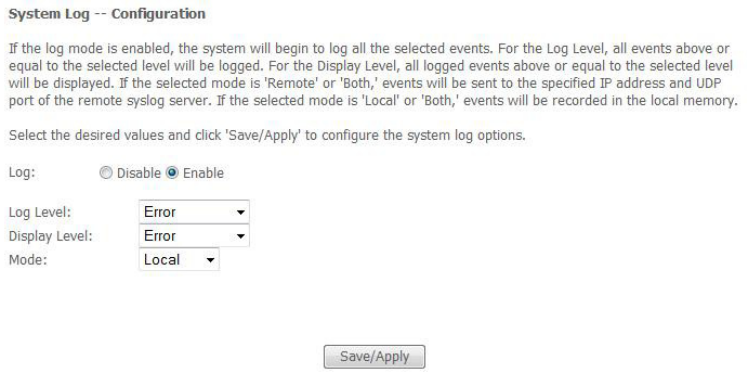
9.2 System Log

The System Log option allows you to view the system events log, or to configure the System Log options. The default setting of system log is disabled. Follow the steps below to enable and view the system log.

1: Click **Configure System Log** to display the following screen.

Status > System Log
The System Log dialog allows you to view the System Log and configure the System Log options.
Click "View System Log" to view the System Log.
Click "Configure System Log" to configure the System Log options.
View System Log
Configure System Log

2: Select from the desired Log options described in the following table, and then click **Save/Apply.**


System Log -- Configuration
If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.
Select the desired values and click 'Save/Apply' to configure the system log options.
Log: Disable Enable
Log Level: Error
Display Level: Error
Mode: Local
Save/Apply

Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, tick Enable and then Apply button.
Log level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the device SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging," which is the lowest critical level. The following log levels are • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice= normal but insignificant condition • Informational= provides information for reference • Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the View System Log screen for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote syslog server or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote syslog server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

3: Click View System Log. The results are displayed as follows.

Date/Time	Facility	Severity	Message
Jan 1 00:00:25	syslog	emerg	BCM96345 started: BusyBox v1.00 (2010.03.26-01:56+0000)
Jan 1 00:00:25	user	debug	syslog: klogd &
Jan 1 00:00:25	user	debug	syslog: sntp -s 0.netcomm.pool.ntp.org -s 1.netcomm.pool.ntp.org -t "Canberra, Melbourne, Sydney" &

9.3 WAN

Select WAN from the Device Info menu to display the status of all configured PVC(s).

Port/VPI/VCI	Shows the values of the ATM Port/VPI/VCI
VLAN Mux	Shows 802.1Q VLAN ID
Con. ID	Shows the connection ID
Category	Shows the ATM service classes
Service	Shows the name for WAN connection
Interface	Shows connection interfaces
Protocol	Shows the connection type (e.g. PPPoE, PPPoA, etc.)
IGMP	Shows the status of the IGMP function
NAT	Enable/Disable Firewall (leave enabled unless advised otherwise by tech support
Firewall	Enable/Disable NAT (leave enabled unless advised otherwise by tech support
QoS	Shows the status of the QoS function
State	Shows the connection state of the WAN connection
Status	Lists the status of the PVC.
IP Address	Shows IP address for WAN interface

9.4 Statistics

This submenu provides statistics for LAN, WAN, ATM and ADSL connections.

NOTE: These statistics refresh every 10 seconds.

9.4.1 LAN Statistics

The Network Statistics screen shows interface statistics for Ethernet and Wireless interfaces. (The Network Statistics screen shows interface statistics of LAN. Eg; Here provides byte transfer, packet transfer, Error and Drop statistics for the LAN interface.)

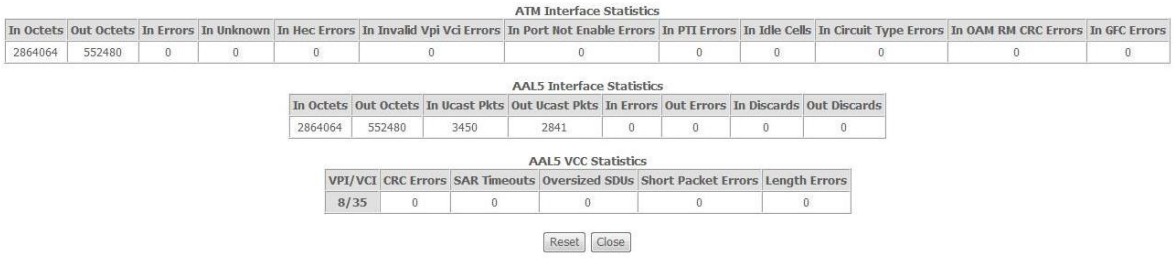
9.4.2 WAN Statistics

WAN statistics screen shows the interface statistics for all WAN connections

Service		Shows the service type
VPI/VCI		Shows the values of the ATM VPI/VCI
Protocol		Shows the connection type
Interface		Shows connection interfaces
Received/ Transmitted	- Bytes	Rx/TX (receive/transmit) packet in Byte
	- Pkts	Rx/TX (receive/transmit) packets
	- Errs	Rx/TX (receive/transmit) packets with errors
	- Drops	Rx/TX (receive/transmit) dropped packets

9.4.3 ATM Statistics

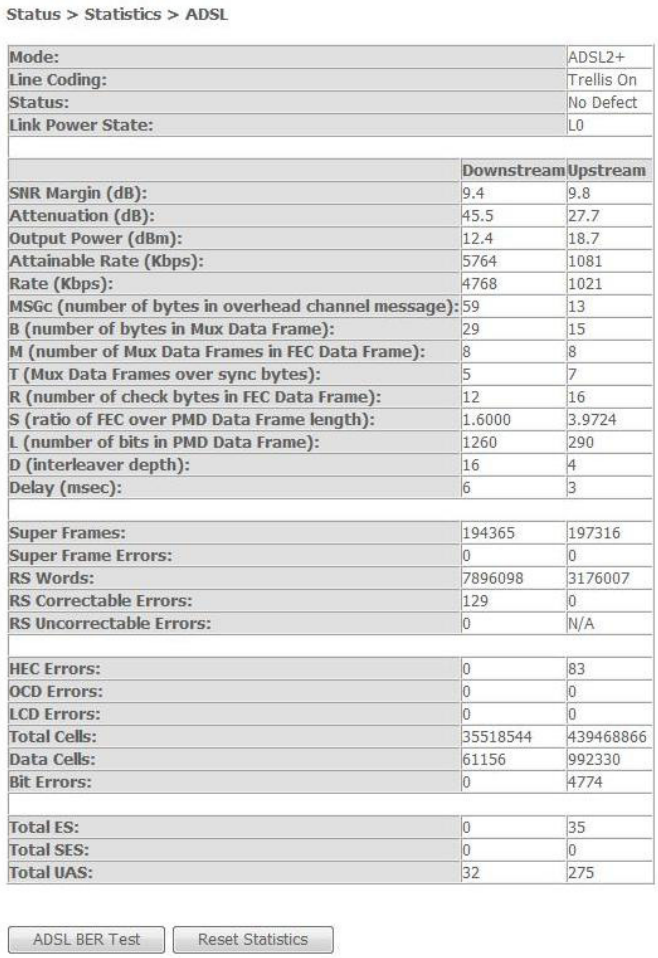
The figure below shows the ATM statistics screen when using ADSL.



Field	Description
In Octets	Number of received octets over the interface
Out Octets	Number of transmitted octets over the interface
In Errors	Number of cells dropped due to uncorrectable HEC errors
In Unknown	Number of received cells discarded during cell header validation, including cells with unrecognized VPI/VCI values, and cells with invalid cell header patterns. If cells with undefined PTI values are discarded, they are also counted here.
In Hec Errors	Number of cells received with an ATM Cell Header HEX error
In Invalid Vpi Vci Errors	Number of cells received with an unregistered VCC address.
In Port Not Enable Errors	Number of cells received on a port that has not been enabled.
In PTI Errors	Number of cells received with an ATM header Payload Type Indicator (PTI) error
In Idle Cells	Number of idle cells received
In Circuit Type Errors	Number of cells received with an illegal circuit type
In OAM RM CRC Errors	Number of OAM and RM cells received with CRC errors
In GFC Errors	Number of cells received with a non-zero GFC.

9.4.4 ADSL Statistics

The following graphic shows the ADSL Network Statistics screen. The **Reset** button (located at the bottom of the screen) can be used to reset statistics. The bit error rate can be tested by clicking the **ADSL BER** Test button.



Status > Statistics > ADSL

Mode:		ADSL2+
Line Coding:		Trellis On
Status:		No Defect
Link Power State:		L0
	Downstream	Upstream
SNR Margin (dB):	9.4	9.8
Attenuation (dB):	45.5	27.7
Output Power (dBm):	12.4	18.7
Attainable Rate (Kbps):	5764	1081
Rate (Kbps):	4768	1021
MSGc (number of bytes in overhead channel message):	59	13
B (number of bytes in Mux Data Frame):	29	15
M (number of Mux Data Frames in FEC Data Frame):	8	8
T (Mux Data Frames over sync bytes):	5	7
R (number of check bytes in FEC Data Frame):	12	16
S (ratio of FEC over PMD Data Frame length):	1.6000	3.9724
L (number of bits in PMD Data Frame):	1260	290
D (interleaver depth):	16	4
Delay (msec):	6	3
Super Frames:	194365	197316
Super Frame Errors:	0	0
RS Words:	7896098	3176007
RS Correctable Errors:	129	0
RS Uncorrectable Errors:	0	N/A
HEC Errors:	0	83
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	35518544	439468866
Data Cells:	61156	992330
Bit Errors:	0	4774
Total ES:	0	35
Total SES:	0	0
Total UAS:	32	275

ADSL BER Test Reset Statistics

Consult the table that follows for field descriptions.

Field	Description
Mode	Line Coding format (e.g. G.dmt, G.lite, T1.413, ADSL2)
Line Coding	Trellis On/Off
Status	Lists the status of the ADSL link
Link Power State	Link output power state.
SNR Margin (dB)	Signal to Noise Ratio (SNR) margin
Attenuation (dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rate.

In G.DMT mode the following section is inserted here.

K	Number of bytes in DMT frame
R	Number of check bytes in RS code word
S	RS code word size in DMT frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

In ADSL2+ mode the following section is inserted here.

MSGc	Number of bytes in overhead channel message
B	Number of bytes in Mux Data Frame
M	Number of Mux Data Frames in FEC Data Frame
T	Max Data Frames over sync bytes
R	Number of check bytes in FEC Data Frame
S	Ratio of FEC over PMD Data Frame length
L	Number of bits in PMD Data Frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

Super Frames	Total number of super frames
Super Frame Errors	Number of super frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

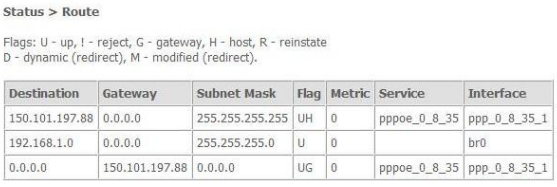
HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of out-of-cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total Cells	Total number of ATM cells (including idle and data cells)
Data Cells	Total number of ATM data cells
Bit Errors	Total number of bit errors

In ADSL2+ mode the following section is inserted here.

Total ES:	Total Number of Errored Seconds
Total SES:	Total Number of Severely Errored Seconds
Total UAS:	Total Number of Unavailable Seconds

9.5 Route

Clicking on 'Status', then 'Route' shows the advanced route configuration of your **NB9WMAXXn**



Status > Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
150.101.197.88	0.0.0.0	255.255.255.255	UH	0	pppoe_0_8_35	ppp_0_8_35_1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	150.101.197.88	0.0.0.0	UG	0	pppoe_0_8_35	ppp_0_8_35_1

9.6 ARP

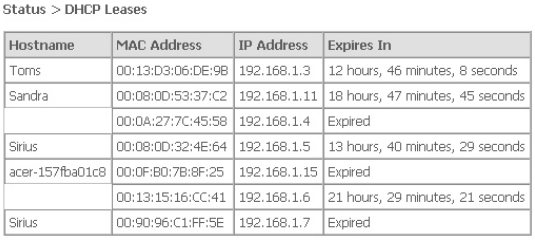
Clicking on 'Status', then 'ARP' shows the current ARP table (The automatic mapping of IP Addresses to MAC addresses) on the **NB9WMAXXn**.

Status > ARP

IP address	Flags	HW Address	Device
192.168.1.3	Complete	00:0D:60:B1:28:BB	br0
192.168.1.2	Complete	00:21:9B:D2:BA:82	br0

9.7 DHCP

Provides summary of DHCP leases provisioned by NB9WMAXXn. Useful source to find client machine MAC addresses.



Status > DHCP Leases

Hostname	MAC Address	IP Address	Expires In
Toms	00:13:D3:06:DE:9B	192.168.1.3	12 hours, 46 minutes, 8 seconds
Sandra	00:08:0D:53:37:C2	192.168.1.11	18 hours, 47 minutes, 45 seconds
	00:0A:27:7C:45:58	192.168.1.4	Expired
Sirius	00:08:0D:32:4E:64	192.168.1.5	13 hours, 40 minutes, 29 seconds
acer-157fba01c8	00:0F:B0:7B:8F:25	192.168.1.15	Expired
	00:13:15:16:CC:41	192.168.1.6	21 hours, 29 minutes, 21 seconds
Sirius	00:90:96:C1:FF:5E	192.168.1.7	Expired

Appendix

Important Additional Information

Appendix A: Legal & Regulatory Information

This manual is copyright. Apart from any fair dealing for the purposes of private study, research, criticism or review, as permitted under the Copyright Act, no part may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm Limited. NetComm Limited accepts no liability or responsibility, for consequences arising from the use of this product.

NetComm Limited reserves the right to change the specifications and operating details of this product without notice.

NetComm is a registered trademark of NetComm Limited.

All other trademarks are acknowledged the property of their respective owners.

Customer Information

ACA (Australian Communications Authority) requires you to be aware of the following information and warnings:

(1) This unit shall be connected to the Telecommunication Network through a line cord which meets the requirements of the ACA TS008 Standard.

(2) This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACA . These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:

- Change the direction or relocate the receiving antenna.
- Increase the separation between this equipment and the receiver.
- Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
- Consult an experienced radio/TV technician for help.

(3) The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

GNU General Public License

This product includes software code that is subject to the GNU General Public License (“GPL”) or GNU Lesser General Public License (“LGPL”). This code is subject to the copyrights of one or more authors and is distributed without any warranty. A copy of this software can be obtained by contacting NetComm Limited on +61 2 9424 2059.

Product Warranty

The warranty is granted on the following conditions:

1. This warranty extends to the original purchaser (you) and is not transferable;
2. This warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. The customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. The cost of transporting product to and from NetComm's nominated premises is your responsibility; and,
5. NetComm does not have any liability or responsibility under this warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour.
6. The customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm recommends that you enable these features to enhance your security.

The warranty is automatically voided if:

1. You, or someone else, use the product, or attempts to use it, other than as specified by NetComm;
2. The fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. The fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. Your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. Your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm; and,
6. The serial number has been defaced or altered in any way or if the serial number plate has been removed.

Limitations of Warranty

The Trade Practices Act 1974 and corresponding State and Territory Fair Trading Acts or legalisation of another Government ("the relevant acts") in certain circumstances imply mandatory conditions and warranties which cannot be excluded. This warranty is in addition to and not in replacement for such conditions and warranties.

To the extent permitted by the Relevant Acts, in relation to your product and any other materials provided with the product ("the Goods") the liability of NetComm under the Relevant Acts is limited at the option of NetComm to:

- Replacement of the Goods; or
- Repair of the Goods; or
- Payment of the cost of replacing the Goods; or
- Payment of the cost of having the Goods repaired.

All NetComm ACN 002 490 486 products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option (refer to packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at

www.netcomm.com.au

NETCOMM LIMITED Head Office
PO Box 1200, Lane Cove NSW 2066 Australia
P: 02 9424 2070 **F:** 02 9424 2010
E: int.sales@netcomm.com.au
W: www.netcommlimited.com.

DYNALINK NZ 12C Te Kea Place, Albany, Auckland,
New Zealand
P: 09 448 5548
F: 09 448 5549
E: sales@dynalink.co.nz
W: www.dynalink.co.nz

Product Warranty

NetComm products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option, via registering your product online at the NetComm website **www.netcommlimited.com**.

Technical Support

If you have any technical difficulties with your product, please refer to the support section of our website.

www.netcomm.com.au/support

Note:NetComm Technical Support for this product only covers the basic installation and features outlined in the Quick Start Guide. For further information regarding the advanced features of this product, please refer to the configuring sections in the User Guide or contact a Network Specialist.

Trademarks and registered trademarks are the property of NetComm Limited or their respective owners. Specifications are subject to change without notice. Images shown may vary slightly from the actual product.